UNITED STATES COPYRIGHT OFFICE

SECTION 1201 RULEMAKING:
Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention

RECOMMENDATION OF THE REGISTER OF COPYRIGHTS

OCTOBER 2015

The Register of Copyrights of the United States of America
United States Copyright Office · 101 Independence Avenue SE · Washington, DC 20559-6000 · (202) 707-8350

October 8, 2015

David Mao
Acting Librarian of Congress
Library of Congress
101 Independence Ave, SE
Washington, DC 20540

Dear Acting Librarian Mao:

Pursuant to my statutory obligation under 17 U.S.C. 1201(a)(l)(C) please find the attached recommendation relating to the rulemaking on exemptions from the prohibition on circumvention of technological measures that control access to copyrighted works.

Respectfully,

Maria A. Pallante
Register of Copyrights and Director
U.S. Copyright Office

cc: Elizabeth A. Pugh, General Counsel, Library of Congress

Section 1201 Rulemaking:
Sixth Triennial Proceeding to Determine
Exemptions to the Prohibition on Circumvention

Recommendation of the Register of Copyrights

TABLE OF CONTENTS

Section 1201 Rulemaking:
Sixth Triennial Proceeding to Determine
Exemptions to the Prohibition on Circumvention

Recommendation of the Register of Copyrights

INTRODUCTION

The Digital Millennium Copyright Act ("DMCA") has played a critical role in the development of the digital marketplace that is a defining feature of modern life. Enacted by Congress in 1998,[1] the DMCA has fostered widespread dissemination and enjoyment of creative works by establishing legal protections for copyrighted content—as well as for the consumers and businesses who wish to access and use it—whether over the internet or through a computer or device.[2]

The section 1201 rulemaking is a key part of the DMCA, striking a balance between copyright and digital technologies. While the DMCA generally prohibits the circumvention of technological measures employed by or on behalf of copyright owners to protect their works (also known as "access controls"), the rulemaking process permits the Librarian of Congress, following a public proceeding conducted by the Copyright Office, to grant limited exceptions every three years to ensure that the public can still engage in fair and other noninfringing uses of works.[3] In accordance with the statute, the Librarian's determination to grant an exemption is based upon the recommendation of the Register of Copyrights, who also consults with the National Telecommunications and Information Administration ("NTIA") of the Department of Commerce.[4]

Revised Rulemaking Procedures

The Register revised the administrative process for this sixth rulemaking proceeding. In prior proceedings, the Copyright Office required proponents to provide complete legal and evidentiary support for their proposals at the outset of the rulemaking process. For this rulemaking, members of the public were instead able to propose exemptions by filing brief petitions containing only basic information. The Office then reviewed and grouped the 44 petition requests into 27 classes and published the proposals, after which proponents and opponents of the proposals had the opportunity to submit written comments offering specific legal and factual support for their respective positions.[5] The Office provided detailed guidance to assist the public during this process,

---

[1] *See generally* DMCA, Pub. L. No. 105-304, 112 Stat. 2860 (1998).

[2] *See* H.R. REP. NO. 105-551, pt. 2, at 22 (1998) ("Commerce Comm. Report").

[3] 17 U.S.C. § 1201(a)(1); *see also* Commerce Comm. Report at 25-26, 35-36.

[4] 17 U.S.C. § 1201(a)(1)(C); *see also* Commerce Comm. Report at 37.

[5] *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 79 Fed. Reg. 73,856, 73,857-59 (Dec. 12, 2014) ("NPRM").

including template forms.[6] During the course of the rulemaking, the Office received nearly 40,000 comments. The written submissions were followed by seven days of public hearings in Los Angeles and Washington, D.C.,[7] at which the Office received testimony from sixty-three witnesses.

Policy Considerations

This sixth triennial rulemaking has been the most extensive and wide-ranging to date and is carefully documented and addressed in the ensuing 403-page Recommendation. As explained, some of the proposed exemptions concern the ability to access and make noninfringing uses of expressive copyrighted works such as motion pictures, video games and e-books, as Congress undoubtedly had in mind when it created the triennial review process. But many other proposals seek to access the copyrighted computer code that now pervades consumer devices. Proponents of these latter classes are not seeking to access software for its creative content, but rather to enable greater functionality of devices ranging from cellphones, tablets and smart TVs to automobiles, tractors and pacemakers. For example, good-faith security researchers seek the ability to circumvent access controls in order to identify and address flaws and malfunctions in the computer programs embedded in consumer products, vehicles and medical devices. Automobile and tractor owners want to access vehicle software to make repairs and modifications. Patients seek access to compilations of data generated by the life-saving medical devices on which they rely. In each of these cases, the prospective users are concerned about violating section 1201.

The discussion of the various proposals that follows richly illustrates both the importance and limitations of the DMCA's anticircumvention rule and triennial rulemaking process. While it is clear that section 1201 has played a critical role in the development of secure platforms for the digital distribution of copyrighted works, it is also the case that the prohibition on circumvention impacts a wide range of consumer activities that have little to do with the consumption of creative content or the core concerns of copyright. Many of the issues that were raised in this proceeding would be more properly debated by Congress or the agencies with primary jurisdiction in the relevant areas. Indeed, the present record indicates that different parts of the Administration have varying views on the wisdom of permitting circumvention for security research or to enable modification of motor vehicles. NTIA has endorsed broad exemptions to facilitate these activities, while the Environmental Protection Agency is opposed, and the Department of Transportation expresses substantial reservations. There are also concerns about circumvention of medical device software. While the Food and

[6] *See id.* at 73,857-58.

[7] *See* Notice of Public Hearings: Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 19,255, 19,255 (Apr. 10, 2015). The hearing agenda is posted at http://copyright.gov/1201/2015/Final_1201_hearing_agenda_20150507.pdf. Transcripts for the hearings are posted at http://copyright.gov/1201/2015/hearing-transcripts. Hearing exhibits are posted at http://copyright.gov/1201/2015/hearing-exhibits.

Drug Administration has raised regulatory concerns concerning the impact of circumvention activities on the devices it regulates, NTIA supports proposed exemptions to allow security testing on medical devices as well as access to the data they generate.

In light of the substantial public safety and environmental concerns raised by government actors and others, the Register is of the view that the Librarian should exercise a degree of caution in adopting exemptions to facilitate security research on consumer goods, motor vehicles and medical devices, as well as for purposes of vehicle repair. The Register appreciates and agrees with NTIA's view that such concerns have "at best a very tenuous nexus to copyright protection."[8] But they are serious issues nevertheless. Accordingly, while the Register generally concurs with NTIA that exemptions should be granted in these areas, the Register nonetheless believes it is appropriate to take the competing concerns of other agencies into consideration. As explained more fully below, the Register is recommending a window of twelve months before exemptions that may implicate public safety and environmental concerns become effective, which will provide an opportunity for the various parts of the federal government, as well as state agencies, to prepare for any impact.

This proceeding points to other policy concerns as well. As in the past, the rulemaking process has highlighted aspects of the Copyright Act that have not kept up with changing technologies. For example, while Congress clearly foresaw the need to facilitate good-faith security research when it enacted a standing exemption for security testing in section 1201(j), the exemption does not seem sufficiently robust in light of the perils of today's connected world.[9] And, as is apparent in the proposal to allow preservation of video games, the exceptions for preservation activities set forth in section 108 appear inadequate to address institutional needs in relation to digital works.[10] The

[8] Letter from Lawrence E. Strickling, Assistant Sec'y for Commc'ns & Info., Nat'l Telecomms. & Info. Admin., U.S. Dep't of Commerce, to Maria A. Pallante, Register of Copyrights and Dir., U.S. Copyright Office ("USCO"), at 4 (Sept. 18, 2015) ("NTIA Letter").

[9] *The Register's Perspective on Copyright Review: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 29, 57 (2015) ("*The Register's Perspective on Copyright Review Hearing*") (statement of Maria A. Pallante, Register of Copyrights and Dir., USCO); *id.* at 57 (statement of Rep. Zoe Lofgren, Member, H. Comm. on the Judiciary) ("I recently met with some researchers, academically based, ... [a]nd they are good guys. They are exploring cybersecurity issues. And to do so, they have to actually do some breaking. And we want them to because we want to find out what the holes are. But they're very concerned. They're a law-abiding group. They don't want to be behind a law violation.").

[10] *Id.* at 20-21 (statement of Maria A. Pallante, Register of Copyrights and Dir., USCO); *see also Preservation and Reuse of Copyrighted Works: Hearing Before the Subcomm. on Courts, Intellectual Prop., and the Internet of the H. Comm. on the Judiciary*, 113th Cong. 2 (2014) (statement of Rep. Jerrold Nadler, Ranking Member, Subcomm. on Courts, Intellectual Prop., and the Internet) ("Recognizing the unique public service mission served by libraries and archives, Congress first enacted section 108 in 1976, allowing these entities a limited exception for preservation, replacement, and research purposes long before technological innovations made it possible to make digital copies of analog works on a mass scale, a process otherwise known as mass digitization."); THE SECTION 108 STUDY GROUP, THE SECTION 108 STUDY GROUP REPORT, at i (2008), *available at* http://www.section108.gov/docs/Sec108StudyGroup Report.pdf.

sixth triennial rulemaking thus soundly affirms Congress's substantial efforts over the past two years to review the Copyright Act and assess where it is in need of updates.[11]

Additionally, as has also been true in the past, a number of proposals essentially seek renewal of existing exemptions—for example, unlocking of cellphones and jailbreaking of smartphones. As the Register suggested in recent testimony before the Judiciary Committee of the House of Representatives, Congress could amend the rulemaking process to create a presumption in favor of renewal when there is no meaningful opposition to the continuation of an exemption.[12] Not only will this lessen the burden on proponents, but it will also allow for a more streamlined rulemaking process. Under current law, the Copyright Office must assess proponents' evidence every three years anew as though the exemption were presented for the first time, even when proponents have in a previous rulemaking made a strong case. When there is an existing exemption, however, the evidence may be weak, incomplete or otherwise inadequate to support the request for renewal, as was the case with the cellphone unlocking proposals in the 2012 proceeding.

Finally, Congress may wish to consider clarifications to section 1201 to ensure that the beneficiaries of exemptions are able to take full advantage of them even if they need assistance from third parties.[13] The anti-trafficking rules set forth in sections 1201(a)(2) and 1201(b) generally prohibit the manufacture and provision of technologies, products or services—or "part[s] thereof"—that are "primarily" designed for purposes of

---

[11] *See* Press Release, H. Comm. on the Judiciary, Chairman Goodlatte Announces Comprehensive Review of Copyright Law (Apr. 24, 2013), *available at* http://judiciary.house.gov/index.cfm/2013/4/chairman goodlatteannouncescomprehensivereviewofcopyrightlaw ("There is little doubt that our copyright system faces new challenges today."); *The Register's Perspective on Copyright Review Hearing* at 7-8 (statement of Maria A. Pallante, Register of Copyrights and Dir., USCO); *The Register's Perspective on Copyright Review Hearing* at 56 (statement of Rep. Zoe Lofgren, Member, H. Comm. on the Judiciary) (noting that "as the [1201] exemptions have proliferated, I think it tells us something about the underlying defect in the statute"); *Chapter 12 of Title 17: Hearing Before the Subcomm. on Courts, Intellectual Prop., and the Internet of the H. Comm. on the Judiciary*, 113th Cong. 64 (2014) (statement of Rep. Bob Goodlatte, Chairman, H. Comm. on the Judiciary) ("As someone who was very active in negotiating all of the DMCA, I am not sure that anyone involved in the drafting would have anticipated some of the TPM uses that have been litigated in court. Such as replacement printer toner cartridges and garage door openers. So I am also interested in ways to better focus Chapter 12 on protecting copyright works from piracy rather than protecting non-copyright industries from competition.").

[12] *The Register's Perspective on Copyright Review Hearing* at 27 (statement of Maria A. Pallante, Register of Copyrights and Dir., USCO).

[13] Section 1201(a)(2) is addressed to technological measures limiting access to works, while section 1201(b) is addressed to technological measures limiting copying of works. *See* 17 U.S.C. § 1201(a)(2), (b). Some technological measures control both access to and copying of works. 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, at 44-47 (June 11, 2010) ("2010 Recommendation") (quoting Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,556, 64,568 (Oct. 27, 2000) ("2000 Final Rule")) (explaining that the Content Scramble System, a TPM that protects DVDs, "is an access control that also (and, arguably, primarily) serves to prevent copying").

circumvention.[14] Any exemption granted by the Librarian on the Register's recommendation may not override these provisions.[15] While the anti-trafficking provisions can curtail bad actors seeking to profit from circumvention by others, they also constrain the ability to allow third parties to offer assistance to exempted users.

Congress adopted a limited clarification on this point in relation to the unlocking of wireless devices in 2014 when it passed the Unlocking Consumer Choice and Wireless Competition Act ("Unlocking Act"), which, among other things, amended section 1201 to permit specified third parties to circumvent technological measures "at the direction of" a cellphone or device owner to enable its use on a different wireless network.[16] The issue of third-party assistance has surfaced again in the current proceeding, as reflected in proposals to allow circumvention "on behalf of" vehicle owners to facilitate repairs or permit access to medical data "at the direction of" the patient. Assistance with these types of activities is not authorized under the 2014 Unlocking Act. Congress may wish to consider another amendment to section 1201 to address these sorts of situations, for example, by expressly allowing the Librarian to adopt exemptions that permit third-party assistance when justified by the record.

Summary of Recommendations

The Librarian has previously adopted five sets of exemptions under section 1201[17] based upon prior Recommendations of the Register.[18] In this sixth triennial

[14] Section 1201(a)(2) provides that "[n]o person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part 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 . . . ." 17 U.S.C. § 1201(a)(2)(A). Section 1201(b) provides that "[n]o person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that . . . is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof . . . ." *Id.* § 1201(b)(1)(A).

[15] *See id.* § 1201(a)(1)(E) ("Neither the exception under subparagraph (B) from the applicability of the prohibition contained in subparagraph (A), nor any determination made in a rulemaking conducted under subparagraph (C), may be used as a defense in any action to enforce any provision of this title other than this paragraph."); *see also* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 79 Fed. Reg. 55,687, 55,688 n.2 (Sept. 17, 2014) ("NOI").

[16] *See* Unlocking Act, Pub. L. No. 113-144, § 2(c), 128 Stat. 1751, 1751-52 (2014) (providing that circumvention "may be initiated . . . by another person at the direction of the owner, or by a provider of a commercial mobile radio service or a commercial mobile data service at the direction of such owner or other person, solely in order to enable such owner or a family member of such owner to connect to a wireless telecommunications network . . . ."). The Unlocking Act, however, provides a narrow fix to the issue of third-party circumvention since the Act applies only in the context of exemptions that permit unlocking of cellphones and other wireless devices. *See* S. REP. NO. 113-212, at 6-7 (2014).

[17] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 77 Fed. Reg. 65,260 (Oct. 26, 2012) ("2012 Final Rule"), *amended by* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Wireless Telephone Handsets, 79 Fed. Reg. 50,552 (Aug. 25, 2014) (codified at 37 C.F.R. § 201.40(b)(3), (c)); Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 75 Fed. Reg. 43,825

proceeding, as discussed more fully below, the Register recommends that the Librarian adopt another set of exemptions covering twenty-two types of uses, as follows:

- Motion pictures (including television programs and videos):
  - For educational uses by college and university instructors and students
  - For educational uses by K-12 instructors and students
  - For educational uses in massive open online courses ("MOOCs")
  - For educational uses in digital and literacy programs offered by libraries, museums and other nonprofits
  - For multimedia e-books offering film analysis
  - For uses in documentary films
  - For uses in noncommercial videos
- Literary works distributed electronically (*i.e.*, e-books), for use with assistive technologies for persons who are blind, visually impaired or have print disabilities
- Computer programs that operate the following types of devices, to allow connection of a used device to an alternative wireless network ("unlocking"):
  - Cellphones
  - Tablets
  - Mobile hotspots
  - Wearable devices (*e.g.*, smartwatches)
- Computer programs that operate the following types of devices, to allow the device to interoperate with or to remove software applications ("jailbreaking"):

(July 27, 2010) ("2010 Final Rule"); Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68,472 (Nov. 27, 2006) ("2006 Final Rule"); Copyright Office, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 68 Fed. Reg. 62,011 (Oct. 31, 2003) ("2003 Final Rule"); 2000 Final Rule, 65 Fed. Reg. 64,556 .

[18] Register of Copyrights, Section 1201 Rulemaking: Fifth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendation of the Register of Copyrights (Oct. 12, 2012) ("2012 Recommendation"); 2010 Recommendation; Recommendation of the Register of Copyrights in RM 2005-11, Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (Nov. 17, 2006) ("2006 Recommendation"); Recommendation of the Register of Copyrights in RM 2002-4, Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (Oct. 27, 2003) ("2003 Recommendation"); 2000 Final Rule, 65 Fed. Reg. 64,556 (Librarian's Final Rule, including the full text of the Register's Recommendation). The Final Rules and the Register's Recommendations can be found at http://www.copyright.gov/1201.

  - Smartphones
  - Tablets and other all-purpose mobile computing devices
  - Smart TVs
- Computer programs that control motorized land vehicles, including farm equipment, for purposes of diagnosis, repair and modification of the vehicle (effective in 12 months)
- Computer programs that operate the following devices and machines, for purposes of good-faith security research (effective in 12 months or, for voting machines, immediately):
  - Devices and machines primarily designed for use by individual consumers, including voting machines
  - Motorized land vehicles
  - Medical devices designed for implantation in patients and corresponding personal monitoring systems
- Video games for which outside server support has been discontinued, to allow individual play by gamers and preservation of games by libraries, archives and museums (as well as necessary jailbreaking of console computer code for preservation uses only)
- Computer programs that operate 3D printers, to allow use of alternative feedstock
- Literary works consisting of compilations of data generated by implanted medical devices and corresponding personal monitoring systems

The Register declines to recommend the following requested exemptions:

- Audiovisual works, for broad-based space-shifting and format-shifting (declined due to lack of legal and factual support for exemption)
- Computer programs in video game consoles, for jailbreaking purposes (declined due to lack of legal and factual support for exemption)
- Literary works distributed electronically (e-books), for space-shifting and format shifting (declined because incomplete record presented)
- Computer programs that operate "consumer machines," for unlocking (declined because incomplete record presented)
- Computer programs that operate dedicated e-book readers, for jailbreaking (declined because incomplete record presented)
- Computer programs consisting of specific music recording software that is no longer supported, to allow continued use of the software (declined because incomplete record presented)

I. LEGAL BACKGROUND

A. Section 1201(a)(1)

Congress enacted the DMCA in 1998 to implement certain provisions of the WIPO Copyright and WIPO Performances and Phonograms Treaties. Among other things, title I of the DMCA, which added a new chapter 12 to title 17 of the U.S. Code, prohibits circumvention of technological measures employed by or on behalf of copyright owners to protect access to their works. In enacting this aspect of the law, Congress observed that technological protection measures ("TPMs") can "support new ways of disseminating copyrighted materials to users, and . . . safeguard the availability of legitimate uses of those materials by individuals."[19]

Section 1201(a)(1) provides in pertinent part that "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under [title 17]." Under the statute, to "circumvent a technological measure" means "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."[20] A technological measure that "effectively controls access to a work" is one that "in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."[21]

As originally drafted, the prohibition in section 1201(a)(1)(A) did not provide for an exemption process.[22] The House of Representatives Committee on Commerce ("the Commerce Committee" or "the Committee") was concerned, however, that the lack of an ability to waive the prohibition might undermine the fair use of copyrighted works.[23] The Committee acknowledged that the growth and development of the internet had had a significant positive impact on the access of students, researchers, consumers, and the public at large to information, and that a "plethora of information, most of it embodied in materials subject to copyright protection, is available to individuals, often for free, that just a few years ago could have been located and acquired only through the expenditure of considerable time, resources, and money."[24] At the same time, the Committee was concerned that "marketplace realities may someday dictate a different outcome, resulting

---

[19] STAFF OF H. COMM. ON THE JUDICIARY, 105TH CONG., SECTION-BY-SECTION ANALYSIS OF H.R. 2281 AS PASSED BY THE UNITED STATES HOUSE OF REPRESENTATIVES ON AUGUST 4, 1998, at 6 (Comm. Print 1998) ("House Manager's Report").

[20] 17 U.S.C. § 1201(a)(3)(A).

[21] *Id.* § 1201(a)(3)(B).

[22] The original version of the bill did provide for certain permanent exemptions, including for library browsing, reverse engineering, and other activities, which were included in section 1201 as finally enacted. *See* S. REP. NO. 105-190, at 13-16 (1998).

[23] Commerce Comm. Report at 35-36.

[24] *Id.*

in less access, rather than more, to copyrighted materials that are important to education, scholarship, and other socially vital endeavors."[25] The Committee thus concluded that it would 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."[26]

Accordingly, the Commerce Committee offered a modification of proposed section 1201 that it characterized as a "'fail-safe' mechanism."[27] The Committee's report noted that "[t]his 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."[28]

As ultimately enacted, the "fail-safe" mechanism in section 1201(a)(1) requires the Librarian of Congress, following a rulemaking proceeding, to publish any class of copyrighted works as to which the Librarian has determined that noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected by the prohibition against circumvention in the succeeding three-year period, thereby exempting that class from the prohibition for that period.[29] The Librarian's determination to grant an exemption is based upon the recommendation of the Register of Copyrights, who conducts the rulemaking proceeding.[30] Congress directed the Register, in turn, to consult with the Assistant Secretary for Communications and Information of the Department of Commerce, who oversees NTIA, in the course of formulating her recommendation.[31] As explained by the Commerce Committee, "[t]he 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."[32]

In keeping with that goal, the primary responsibility of the Register and the Librarian in the rulemaking proceeding is to assess whether the implementation of access controls impairs the ability of individuals to make noninfringing uses of copyrighted works within the meaning of section 1201(a)(1). To do this, the Register develops a

---

[25] *Id.* at 36.

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *See* 17 U.S.C. § 1201(a)(1).

[30] *Id.* § 1201(a)(1)(C); H.R. REP. NO. 105-796, at 64 (1998) ("Conference Report").

[31] 17 U.S.C. § 1201(a)(1)(C). Exemptions adopted by rule under section 1201(a)(1)(C) apply only to the prohibition on circumventing technological measures that control "access" to copyrighted works, *e.g.*, decryption or hacking of access controls such as passwords.

[32] *See* Commerce Comm. Report at 37.

comprehensive administrative record using information submitted by interested parties, and makes recommendations to the Librarian concerning whether exemptions are warranted based on that record.[33]

Under the statutory framework, the Librarian, and thus the Register, must consider "(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."[34] As noted above, the Register must also consult with the Assistant Secretary, who oversees NTIA, and report and comment on his views, in providing her Recommendation. Upon receipt of the Recommendation, the Librarian is responsible for promulgating the final rule setting forth any exempted classes of works.

B. Relationship to Other Provisions of Section 1201 and Other Laws

Significantly, exemptions adopted by rule under section 1201(a)(1) apply only to the conduct of circumventing a technological measure that controls "access" to a copyrighted work. Other parts of section 1201, by contrast, address the manufacture and provision of—or "trafficking" in—products and services primarily designed for purposes of circumvention. Section 1201(a)(2) bars trafficking in products and services that are used to circumvent technological measures that control *access* to copyrighted works (for example, a password needed to open a media file),[35] while section 1201(b) bars trafficking in products and services used to circumvent technological measures that protect the *exclusive rights* of the copyright owners in their works (for example, technology that prevents the work from being reproduced).[36] The Librarian of Congress has no authority to adopt exemptions for the anti-trafficking prohibitions contained in subsections (a)(2) or (b) of section 1201.[37]

---

[33] *See* Conference Report at 64 ("[A]s is typical with other rulemaking under title 17, and in recognition of the expertise of the Copyright Office, the Register of Copyrights will conduct the rulemaking, including providing notice of the rulemaking, seeking comments from the public, consulting with the Assistant Secretary for Communications and Information of the Department of Commerce and any other agencies that are deemed appropriate, and recommending final regulations in the report to the Librarian.").

[34] 17 U.S.C. § 1201(a)(1)(C).

[35] *Id.* § 1201(a)(2).

[36] *Id.* § 1201(b).

[37] *See id.* § 1201(a)(1)(E) ("Neither the exception under subparagraph (B) from the applicability of the prohibition contained in subparagraph (A), nor any determination made in a rulemaking conducted under subparagraph (C), may be used as a defense in any action to enforce any provision of this title other than this paragraph."). However, the statute contains exemptions from the trafficking prohibitions for certain limited uses, such as reverse engineering or encryption research. *See id.* § 1201(f)(2), (g)(4).

More broadly, activities conducted under the regulatory exemptions must still comply with other applicable laws, including non-copyright provisions. Thus, while an exemption may specifically reference other laws of particular concern, any activities conducted under an exemption must be otherwise lawful.

Also significant is the fact that the statute contains certain permanent exemptions to permit specified uses. These are:

- Section 1201(d), which exempts certain activities of nonprofit libraries, archives, and educational institutions from the circumvention ban in section 1201(a)(1) (but not the anti-trafficking provisions of section 1201(a)(2) and (b)), so that they can "make a good faith determination of whether to acquire a copy of that work for the sole purpose of engaging in conduct permitted under this title."

- Section 1201(e), which exempts "any lawfully authorized investigative, protective, information security, or intelligence activity" of the state or federal government from the anticircumvention and anti-trafficking provisions in section 1201(a)(1), (a)(2), and (b).

- Section 1201(f), which exempts certain "reverse engineering" activities from section 1201(a)(1), (a)(2), and (b), "for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs."

- Section 1201(g), which exempts certain "encryption research" from section 1201(a)(1) and (2) (but not 1201(b)).

- Section 1201(h), which permits courts, in applying section 1201(a)(1) and (2) to a "component or part," to consider whether the component or part is needed to "prevent the access of minors to material on the Internet."

- Section 1201(i), which exempts certain acts of circumvention "solely for the purpose of preventing the collection or dissemination of personally identifying information about a natural person who seeks to gain access to the work protected" from section 1201(a)(1).

- Section 1201(j), which exempts certain acts of "security testing" from section 1201(a)(1) and (2).

C. The Unlocking Consumer Choice and Wireless Competition Act

In 2014, Congress enacted the Unlocking Act, effective as of August 1, 2014.[38] The Unlocking Act did three things. First, it changed the exemption adopted in the last triennial proceeding allowing circumvention of technological measures to enable certain wireless telephone handsets to connect to wireless communication networks—a process commonly known as "cellphone unlocking"—by substituting a broader version of the exemption adopted by the Librarian in 2010[39] for the 2012 version.[40] At the same time, the language of the Unlocking Act makes clear that the Register is to consider any future proposal for a cellphone unlocking exemption according to the usual triennial rulemaking process.[41]

Second, the legislation provides that the circumvention permitted under the reinstated 2010 exemption, as well as any future exemptions to permit wireless telephone handsets or other wireless devices to connect to wireless telecommunications networks, may be initiated by the owner of the handset or device, by another person at the direction of the owner, or by a provider of commercial mobile radio or data services to enable such owner or a family member to connect to a wireless network when authorized by the network operator.[42] This directive is permanent, and is now reflected in the relevant regulations.[43] Accordingly, circumvention under any future "unlocking" exemption for

[38] *See* Unlocking Act, Pub. L. No. 113-144. Subsequently, the Librarian adopted regulatory amendments to reflect the new legislation. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Wireless Telephone Handsets, 79 Fed. Reg. 50,552.

[39] *See* Unlocking Act § 2(a). Although it commenced in 2008, the fourth triennial rulemaking did not conclude until 2010. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 73 Fed. Reg. 79,425 (Dec. 29, 2008); 2010 Final Rule, 75 Fed. Reg. at 43,827.

[40] The 2010 rule allowed unlocking of cellphones initiated by the owner of the copy of the handset computer program in order to connect to a wireless network in an authorized manner. 2010 Final Rule, 75 Fed. Reg. at 43,839. Based on the insufficient record put forth by proponents in the 2012 rulemaking proceeding, the Librarian did not extend the exemption with respect to new phones acquired after January 26, 2013 (90 days after the rule went into effect), but permitted the unlocking of older, or "legacy," phones. 2012 Final Rule, 77 Fed. Reg. at 65,264-66. Congress overturned the outcome and enacted the Unlocking Act after public calls for a broader exemption than provided in the 2012 rule. *See Making Unlocking Cell Phones Legal*, WE THE PEOPLE, https://petitions.whitehouse.gov/petition/make-unlocking-cell-phones-legal/1g9KhZG7 (last updated July 25, 2014).

[41] *See* Unlocking Act § 2(c)(2) (referencing the possibility of a new cellphone unlocking exemption adopted "after the date of enactment" of the Unlocking Act); *id.* § 2(d)(2)("Nothing in this Act alters, or shall be construed to alter, the authority of the Librarian of Congress under section 1201(a)(1) of title 17, United States Code.").

[42] *Id.* § 2(a), (c).

[43] *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Wireless Telephone Handsets, 79 Fed. Reg. at 50,554; *see also* 37 C.F.R. § 201.40(c) ("To the extent authorized under paragraph (b) of this section, the circumvention of a technological measure that restricts wireless telephone handsets or other wireless devices from connecting to a wireless telecommunications network may be initiated by the owner of any such handset or other device, by another person at the direction of the owner, or by a provider of a commercial mobile radio service or a commercial mobile data service at the direction

wireless telephone handsets and other wireless devices adopted by the Librarian may be initiated by the persons Congress identified in the Unlocking Act.

Third, the legislation directs the Librarian of Congress to consider as part of the current triennial proceeding whether to "extend" the cellphone unlocking exemption "to include any other category of wireless devices in addition to wireless telephone handsets" based upon the Recommendation of the Register of Copyrights, who in turn is to consult with the Assistant Secretary.[44] This provision does not alter or expand the Librarian's authority to grant exemptions under section 1201(a)(1), but merely directs the Librarian to exercise his existing regulatory authority to consider the adoption of an exemption for other wireless devices. Accordingly, as part of this rulemaking proceeding, the Copyright Office solicited and has evaluated several proposed unlocking exemptions for devices other than cellphones, as addressed in Proposed Classes 12 through 15 below.

D. Rulemaking Standards

In adopting the DMCA, Congress imposed legal and evidentiary requirements for the section 1201 rulemaking proceeding, as discussed below.

1. Burden of Proof

Those who seek an exemption from the prohibition on circumvention bear the burden of establishing that the requirements for granting an exemption have been satisfied. In enacting the DMCA, Congress explained that the "prohibition [of section 1201(a)(1)] is presumed to apply to any and all kinds of works" until the Librarian determines that the requirements for the adoption of an exemption have been met with respect to a particular class of works.[45] In other words, the prohibition against circumvention applies unless and until the Librarian determines 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 . . . in their ability to make noninfringing uses under this title of a particular class of copyrighted works."[46]

Congress' approach to the section 1201 process reflects general principles of agency rulemaking under the Administrative Procedure Act ("APA").[47] In keeping with

---

of such owner or other person, solely in order to enable such owner or a family member of such owner to connect to a wireless telecommunications network, when such connection is authorized by the operator of such network.").

[44] Unlocking Act § 2(b).

[45] Commerce Comm. Report at 37.

[46] 17 U.S.C. § 1201(a)(1)(C).

[47] Congress indicated that the rulemaking under section 1201(a)(1) should be conducted "as is typical with other rulemaking under title 17," to which the APA applies. *See* Conference Report at 64; 17 U.S.C. § 701(e) ("Except as provided by section 706(b) and the regulations issued thereunder, all actions taken by the Register of Copyrights under this title are subject to the provisions of the Administrative Procedure Act of June 11, 1946, as amended . . . .").

this approach, as the Copyright Office has previously explained, the proponent of an exemption must show by a preponderance of the evidence that the harmful impact on noninfringing uses of copyrighted works "is more likely than not."[48] This requirement stems from the statute, which requires a demonstration that users "*are*, or *are likely to be*," adversely affected by the prohibition on circumvention.[49] The APA provides that a rule may not be issued pursuant to formal agency rulemaking "except on consideration of the whole record or those parts thereof cited by a party and supported by and in accordance with the *reliable, probative, and substantial* evidence."[50]

2. *De Novo* Consideration of Exemptions

Congress made clear in enacting the DMCA that the basis for an exemption must be established *de novo* in each triennial proceeding.[51] As Congress stressed, "[t]he regulatory prohibition [of section 1201(a)(1)] is presumed to apply to any and all kinds of works, including those as to which a waiver of applicability was previously in effect, *unless, and until*, the [Librarian] makes a *new* determination that the adverse impact criteria have been met with respect to a particular class and therefore issues a *new* waiver."[52] Accordingly, the fact that an exemption has been previously adopted creates no presumption that readoption is appropriate. This means that a proponent may not simply rely on the fact that the Register has recommended an exemption in the past, but must instead produce relevant evidence in each rulemaking to justify the continuation of the exemption.

That said, however, where a proponent is seeking the readoption of an existing exemption, it may attempt to satisfy its burden by demonstrating that the conditions that led to the adoption of the prior exemption continue to exist today (or that new conditions exist to justify the exemption). This could include, for instance, a showing that the cessation of an exemption will adversely impact users' ability to make noninfringing uses of the class of works covered by the existing exemption. Assuming the proponent succeeds in making such a demonstration, it is incumbent upon any opponent of that exemption to rebut such evidence by showing that the exemption is no longer justified.

3. Adverse Effects on Noninfringing Uses

Proponents who seek to have the Librarian exempt a particular class of works

---

[48] 2010 Recommendation at 10. Under the APA, "[e]xcept as otherwise provided by statute, the proponent of a rule or order has the burden of proof." 5 U.S.C. § 556(d).

[49] 17 U.S.C. § 1201(a)(1)(B) (emphases added).

[50] *See* 5 U.S.C. § 556(d) (emphasis added); *see also Steadman v. Securities and Exchange Comm'n*, 450 U.S. 91, 102 (1981) (holding that the APA "was intended to establish a standard of proof and that the standard adopted is the traditional preponderance-of-the-evidence standard").

[51] *See* Commerce Comm. Report at 37 (explaining that for every rulemaking, "the assessment of adverse impacts on particular categories of works is to be determined de novo").

[52] *Id.* (emphases added).

from section 1201(a)(1)'s prohibition on circumvention must show: (1) that uses affected by the prohibition on circumvention are or are likely to be noninfringing; and (2) that as a result of a technological measure controlling access to a copyrighted work, the prohibition is causing, or in the next three years is likely to cause, an adverse impact on those uses.[53] These requirements are further explained below. The Register also considers potential exemptions under the statutory factors set forth in section 1201(a)(1)(C), also discussed below.

a. Noninfringing Uses

As noted above, Congress believed that it is important to protect noninfringing uses. There are several types of noninfringing uses that could be affected by the prohibition of section 1201(a)(1), including fair use (delineated in section 107), certain educational uses (section 110), and certain uses of computer programs (section 117).

The Register will look to the Copyright Act and relevant judicial precedents when analyzing whether a proposed use is likely to be noninfringing. The statutory language requires that the use *is* or *is likely* to be noninfringing, not merely that the use might plausibly be considered noninfringing.[54] As the Register has indicated previously, there is no "rule of doubt" favoring an exemption when it is unclear that a particular use is a fair or otherwise noninfringing use.[55] Thus, a proponent must show more than that a particular use *could* be noninfringing. Rather, the proponent must establish that the proposed use is likely to qualify as noninfringing under relevant law. And, as noted above, the burden of proving that a particular use is or is likely to be noninfringing belongs to the proponent.

b. Adverse Effects

The second requirement is a showing that users of the class of copyrighted works currently are, or are likely in the ensuing three-year period to be, adversely affected by the prohibition against circumvention.[56] In weighing adverse effects, the Register must assess, in particular, "whether the prevalence of . . . 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."[57]

Congress stressed that the "main focus of the rulemaking proceeding" should be on whether a "substantial diminution" of the availability of works for noninfringing uses is "*actually occurring*" in the marketplace.[58] To prove the existence of adverse effects, it

[53] *See* 17 U.S.C. § 1201(a)(1)(B); *see also* 2012 Recommendation at 6.

[54] *See* 17 U.S.C. § 1201(a)(1)(C); *see also* 2012 Recommendation at 6.

[55] *See* 2012 Recommendation at 7.

[56] 17 U.S.C. § 1201(a)(1)(C).

[57] Commerce Comm. Report at 37.

[58] House Manager's Report at 6 (emphasis in original).

is necessary to demonstrate "distinct, verifiable and measurable impacts" occurring in the marketplace, as exemptions "should not be based upon *de minimis* impacts."[59] Thus, "mere inconveniences" or "individual cases" do not satisfy the rulemaking standard.[60]

To the extent that a proponent is relying on claimed future impacts rather than existing impacts, the statute requires the proponent to establish that such future adverse impacts are "*likely*."[61] An exemption may be based upon anticipated, rather than actual, adverse impacts "only in extraordinary circumstances in which the evidence of likelihood of future adverse impact during that time period is highly specific, strong and persuasive."[62]

The proponent must also demonstrate that the TPM is the *cause* of the claimed adverse impact. "Adverse impacts that flow from other sources, or that are not clearly attributable to implementation of a technological protection measure, are outside the scope of the rulemaking."[63] For instance, adverse effects stemming from "marketplace trends, other technological developments, or changes in the roles of libraries, distributors or other intermediaries" are not cognizable harms under the statute.[64]

4. Statutory Factors

In conducting the rulemaking, the Librarian must also examine the statutory factors listed in section 1201(a)(1)(C). Those factors are: "(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."[65] In some cases, weighing these factors requires the consideration of the benefits that the technological measure brings with respect to the overall creation and dissemination of works in the marketplace, in addition to any negative impact. As Congress explained, "the rulemaking proceedings should consider the positive as well as the adverse effects of these technologies on the availability of copyrighted materials."[66]

[59] Commerce Comm. Report at 37.

[60] House Manager's Report at 6.

[61] 17 U.S.C. § 1201(a)(1)(B), (C) (emphasis added).

[62] House Manager's Report at 6.

[63] Commerce Comm. Report at 37.

[64] House Manager's Report at 6.

[65] 17 U.S.C. § 1201(a)(1)(C).

[66] House Manager's Report at 6.

5. Defining a Class

Section 1201(a)(1) specifies that the exemption adopted as part of this rulemaking must be defined based on "a particular *class* of works."[67] Thus, a major focus of the rulemaking proceeding is how to define the "class" of works for purposes of the exemption. The starting point for any definition of a "particular class" under section 1201(a)(1) is the list of categories appearing in section 102 of title 17, such as literary works, musical works, and sound recordings.[68] But, as Congress made clear, "the 'particular class of copyrighted works' [is intended to] be a *narrow and focused subset* of the broad categories of works . . . identified in section 102 of the Copyright Act."[69] For example, while the category of "literary works" under section 102(a)(1) "embraces both prose creations such as journals, periodicals or books, and computer programs of all kinds," Congress explained that "[i]t is exceedingly unlikely that the impact of the prohibition on circumvention of access control technologies will be the same for scientific journals as it is for computer operating systems."[70] Thus, "these two categories of works, while both 'literary works,' do not constitute a single 'particular class' for purposes of" section 1201(a)(1).[71]

At the same time, Congress emphasized that the Librarian "should not draw the boundaries of 'particular classes' too narrowly."[72] Thus, while the category of "motion pictures and other audiovisual works" in section 102 "may appropriately be subdivided, for purposes of the rulemaking, into classes such as 'motion pictures,' 'television programs,' and other rubrics of similar breadth," Congress made clear that it would be inappropriate "to subdivide overly narrowly into particular genres of motion pictures, such as Westerns, comedies, or live action dramas."[73]

The determination of the appropriate scope of a "class of works" recommended for exemption may also take into account the adverse effects an exemption may have on the market for or value of copyrighted works. 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. Defining an exemption *solely* by reference to the medium on which a work may appear, or the access control measures applied to a work, however, would be inconsistent with Congress's intent in directing the Register and Librarian to define a "particular class" of "works."[74]

---

[67] *See* 17 U.S.C. § 1201(a)(1)(B) (emphasis added).

[68] House Manager's Report at 7.

[69] Commerce Comm. Report at 38 (emphasis added).

[70] House Manager's Report at 7.

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] *See* 2006 Recommendation at 9-10, 15-20.

In the earliest rulemakings, consistent with the records in those proceedings, the Register rejected proposals to classify works by reference to the type of user or use (for example, libraries, or scholarly research).[75] In the 2006 proceeding, however, the Register concluded, based on 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 subcategory thereof may be additionally refined not only by reference to the medium on which the works are distributed, or the particular access controls at issue, but also by reference to the particular type of use and/or user to which the exemption will apply.[76] The Register determined that "it can be appropriate to refine a class by reference to the use or user in order to remedy the adverse effect of the prohibition and to limit the adverse consequences of an exemption."[77]

In sum, "[d]eciding 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 based upon the law and facts developed in the proceeding.[78] Accordingly, the Register will look to the specific record before her to assess the proper scope of the class for a recommended exemption.

[75] *See, e.g.*, 2000 Final Rule, 65 Fed. Reg. at 64,560-61.

[76] 2006 Recommendation at 10.

[77] *Id.* at 19.

[78] House Manager's Report at 7.

II. HISTORY OF SIXTH TRIENNIAL PROCEEDING

In this triennial rulemaking, after consulting with interested members of the public and NTIA, the Register adjusted the administrative process that has been used in prior rulemakings, including the last triennial proceeding.[79] In earlier proceedings, the Copyright Office initiated the rulemaking process by calling for the public to submit proposals for exemptions.[80] Notably, the Office required proponents to provide complete legal and evidentiary support for their proposals at the outset of the rulemaking process, in the proponents' initial submissions.[81] After receiving those submissions, the Office then published a notice of proposed rulemaking describing the proposals and inviting interested parties to submit initial comments (and, later, reply comments) both in support of and in opposition to those proposals.[82] Although the Office offered general information concerning legal and evidentiary requirements, it did not provide more specific guidance concerning the individual proposals before the submission of written comments. The Office then held public hearings to explore the proposed exemptions,[83] and sometimes issued follow-up questions to participants after the hearings.[84]

In the present rulemaking, the Copyright Office implemented several procedural changes to make the process more accessible and understandable to the public, allow greater opportunity for participants to coordinate their efforts, encourage participants to submit effective factual and legal support for their positions, and reduce administrative burdens on both the participants and the Office.

On September 17, 2014, the Copyright Office published a Notice of Inquiry ("NOI") in the Federal Register to initiate the sixth triennial rulemaking proceeding.[85] The NOI invited interested parties to submit "petitions for proposed exemptions" that set forth the essential elements of the exemption.[86] In a departure from prior rulemakings, the Office did not require the proponent of an exemption to deliver the complete legal and

---

[79] *See generally* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 76 Fed. Reg. 60,398 (Sept. 29, 2011).

[80] *See id.* at 60,403-04.

[81] *See id.* at 60,403 (stressing that "[p]roponents should present their *entire* case in their initial comments" and explaining that "the best evidence in support of an exemption would consist of concrete examples or specific instances" of adverse effects on noninfringing uses).

[82] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 76 Fed. Reg. 78,866, 78,868 (Dec. 20, 2011) (asking for "additional factual information that would assist the Office in assessing whether a Proposed Class is warranted for exemption and, if it is, how such a class already proposed should be properly tailored").

[83] *See* Notice of Public Hearings: Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 77 Fed. Reg. 15,327 (Mar. 15, 2012).

[84] The post-hearing questions and responses for the prior rulemaking can be found on the Copyright Office's website at http://copyright.gov/1201/2012/responses.

[85] NOI, 79 Fed. Reg. 55,687.

[86] *Id.* at 55,692-93.

evidentiary basis for its proposal with its initial submission. Instead, the purpose of the petition was to provide the Office and others with basic information regarding the essential elements of the proposed exemption, both to confirm that the threshold requirements of section 1201(a) could be met, and to aid the Office in describing the proposal for the next, more substantive, phase of the rulemaking proceeding.[87] The Office provided detailed suggestions concerning the content of the petitions, and a recommended form for submitters to use.[88] The Office received forty-four petitions for proposed exemptions in response to the NOI, which were posted on the Copyright Office website.[89]

Next, on December 12, 2014, the Office issued a Notice of Proposed Rulemaking ("NPRM") that reviewed and grouped the proposed exemptions set forth in the petitions.[90] In the NPRM, the Copyright Office concluded that three of the petitions sought exemptions that could not be granted as a matter of law, and declined to put those proposals forward for public comment.[91] Each of these petitions sought to permit circumvention of any and all TPMs that constituted digital rights management ("DRM") with respect to unspecified types of copyrighted works for the purpose of engaging in unidentified personal and/or consumer uses.[92] As the Office noted—and as explained above—section 1201(a)(1) requires that "any exemptions adopted as part of this rulemaking must be defined based on 'a *particular class* of works,'" which legislative history characterizes as "'a *narrow and focused subset* of the broad categories of works . . . identified in Section 102 of the Copyright Act.'"[93] The Office thus concluded that "the sweeping type of exemption proposed by these three petitions" could not be granted consistent with the standards of section 1201(a)(1).[94]

In the NPRM, the Office grouped the remaining proposed exemptions into twenty-seven proposed classes of works.[95] In some cases, overlapping proposals were merged into a single combined proposed class. In other cases, individual proposals that encompassed multiple proposed uses were subdivided into multiple classes to aid in the process of review. The Office then provided detailed guidance on the submission of

[87] *Id.* at 55,692.

[88] *Id.*

[89] Petitions received in response to the NOI are posted at http://copyright.gov/1201/2014/petitions. References to these petitions in this Recommendation are by party name (abbreviated where appropriate), followed by subject matter where the party has submitted multiple petitions, followed by "Pet." (*e.g.*, EFF/OTW Disc Remix Pet.).

[90] NPRM, 79 Fed. Reg. at 73,859.

[91] *Id.*

[92] *Id.*

[93] *Id.* (emphases added) (quoting 17 U.S.C. § 1201(a)(1)(B); Commerce Comm. Report at 38).

[94] *Id.*

[95] *See generally id.* at 73,859-71.

comments, including short- and long-form comment templates.[96] In another departure from prior rulemakings, the NPRM also identified a number of specific legal and factual areas of interest with respect to each proposed class, and encouraged commenters to address those issues in the course of their written comments.[97]

The Office also made two refinements to the structure for the written comment phase to encourage a more organized and complete administrative record. First, commenters were required to provide a separate submission for each proposed class during each stage of the public comment period.[98] The Office imposed this requirement to ensure a manageable record in light of the anticipated number of submissions.[99] As the Office explained in the NOI, in past rulemakings "submitters sometimes combined their views on multiple proposals in a single filing, making it difficult and time-consuming for other participants and the Office to sort out which arguments and evidence pertained to which."[100] The Office believed that "requiring separate submissions for each proposed exemption [would] help both participants and the Office keep better track of the record for each proposed exemption."[101] As the proceeding has progressed, the Office has in fact found this to be the case.

Second, in the past, each round of the written comment phase following the initial petitions was open to all potential commenters, whether in support or opposition, which made it challenging for opponents to respond to points being made by proponents, and vice versa. For this rulemaking, the Office divided the written comment phase into three rounds. The first round following the submission of petitions was limited to proponents and members of the public who supported the adoption of a proposed exemption, as well as those who neither supported nor opposed an exemption but sought only to share pertinent information about a specific proposal.[102] The second round of public comment was limited to those who opposed an exemption.[103] The third round was again limited to

[96] *See id.* at 73,858.

[97] *See id.* at 73,859.

[98] *See id.* at 73,857; *see also* NOI, 79 Fed. Reg. at 55,693.

[99] NOI, 79 Fed. Reg. at 55,693.

[100] *Id.* at 55,692. A few commenters submitted general comments addressing overarching issues applicable to multiple classes, including whether the DMCA should restrict consumer uses of lawfully acquired goods, suggesting interpretations of various statutory provisions of section 1201, or proposing procedures for confidential evidentiary submissions. *See* Owners' Rights Initiative General Comments; New America's Open Technology Institute General Comments; Public Knowledge General Comments. The Register has incorporated these comments as appropriate into her analysis.

[101] NOI, 79 Fed. Reg. at 55,692.

[102] Comments received in the first round are posted at http://copyright.gov/1201/2015/comments-020615. References to these comments in this Recommendation are by party name (abbreviated where appropriate), followed by class number where the party has submitted comments for multiple classes, followed by "Supp." (*e.g.*, MLA Class 1 Supp.).

proponents, supporters and neutral parties, in each case who sought to reply to points made in the earlier rounds of comments.[104]

The Office received nearly 40,000 comments in response to the NPRM, the vast majority of which consisted of relatively short statements of support or opposition without substantial legal argument or supporting evidence. As permitted under the Office's instructions, a number of the longer submissions included multimedia evidence to illustrate points made in the written comments.

After receiving and studying the written comments, the Office held seven days of public hearings: in Los Angeles, at the UCLA School of Law, from May 19th to 21st, 2015; and in Washington, D.C., at the Library of Congress, from May 26th to 29th, 2015.[105] The Office heard testimony from sixty-three witnesses at the hearings, and received additional multimedia evidence.[106] After the hearings, the Office issued a number of follow-up questions to participants, and received responses that have been made part of the administrative record.[107]

As observed by various commenting parties, certain of the proposed exemptions—Proposed Classes 21 and 22, for software installed on automobiles and farm equipment for purposes of diagnosis, repair, and modification and security research, and Proposed Class 27, for software installed on medical devices for purposes of access to patient data and for security research—present issues potentially of concern to DOT,

---

[103] Comments received in the second round are posted at http://copyright.gov/1201/2015/comments-032715. References to these comments in this Recommendation are by party name (abbreviated where appropriate), followed by class number where the party has submitted comments for multiple classes, followed by "Opp'n" (*e.g.*, Joint Creators Class 7 Opp'n).

[104] Reply comments are posted at http://copyright.gov/1201/2015/reply-comments-050115. References to these comments in this Recommendation are by party name (abbreviated where appropriate), followed by class number where the party has submitted comments for multiple classes, followed by "Reply" (*e.g.*, Public Knowledge Class 27 Reply).

[105] *See* Notice of Public Hearings: Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 19,255 (Apr. 10, 2015). The hearing agendas are posted at http://copyright.gov/1201/2015/Final_1201_hearing_agenda_20150507.pdf.

[106] Transcripts for the hearings are posted at http://copyright.gov/1201/2015/hearing-transcripts. Hearing exhibits are posted at http://copyright.gov/1201/2015/hearing-exhibits. At the hearing for Proposed Class 21 (covering vehicle software – diagnosis, repair or modification), opponents submitted additional written materials, and the Office provided the opportunity for others to respond after the hearing. That additional written material and responses are posted at http://copyright.gov/1201/2015/class21.

[107] The post-hearing questions are posted at http://copyright.gov/1201/2015/post-hearing. References to these questions in this Recommendation are by "Post-Hearing Questions to," followed by class number, followed by "Witnesses," followed by the date (*e.g.*, Post-Hearing Questions to Class 6 Witnesses (June 3, 2015)). The responses to the post-hearing questions are posted at http://copyright.gov/1201/2015/post-hearing/answers. References to these responses in this Recommendation are by party name (abbreviated where appropriate), followed by class number where the party has submitted responses for multiple classes, followed by "Post-Hearing Resp." (*e.g.*, Joint Creators Class 3 Post-Hearing Resp.).

EPA, and FDA (and perhaps other regulatory agencies as well).[108] The Copyright Office therefore sent letters to DOT, EPA, and FDA informing them of the pendency of the rulemaking proceeding in case they wished to comment on the proposals. In response to these letters, the Office received responses from those agencies, and also from the California Air Resources Board, which are also included in the record.[109]

Throughout this triennial proceeding, as required under section 1201(a)(1), the Register has consulted with NTIA. In addition to providing procedural and substantive input throughout the rulemaking process, NTIA was represented along with Copyright Office staff at the public hearings held in Los Angeles and Washington, D.C. NTIA formally communicated its views on each of the proposed exemptions in a letter delivered to the Register on September 18, 2015.[110] A discussion of NTIA's substantive analysis of particular proposals is presented in the relevant sections of this Recommendation.

[108] *See, e.g.*, Association of Equipment Manufacturers Class 21 Opp'n at 1; Intellectual Property Owners Association Class 27 Opp'n at 2-3.

[109] The Office's letters to those agencies, and the agencies' responses, are posted at http://copyright.gov/1201/2015/USCO-letters.

[110] NTIA Letter at 1.

III. DISCUSSION

A. Proposed Classes 1 to 7: Audiovisual Works – Educational and Derivative Uses

1. Proposals

Proposed Classes 1 through 7 would allow circumvention of lawfully made and acquired motion pictures and, in some cases, other audiovisual works, protected by various access controls, where the person engaging in circumvention seeks to engage in a noninfringing use. Prior rulemakings have granted exemptions relating to uses of motion picture excerpts for commentary, criticism, and educational uses by college and university faculty and staff and by kindergarten through twelfth-grade educators, as well as for derivative uses of excerpts in noncommercial videos, documentary films, and nonfiction multimedia e-books offering film analysis.[111] The current petitions seek to readopt and to some extent expand those previously granted exemptions to accommodate additional technologies, such as Blu-ray discs, or to include new users or types of uses, such as for fictional films or uses by museums, libraries, and nonprofits, or students and faculty participating in massive open online courses ("MOOCs").

The NPRM grouped these proposals into seven classes. The NPRM described Proposed Class 1 as follows:

> Proposed Class 1: This proposed class would allow college and university faculty and students to circumvent access controls on lawfully made and acquired motion pictures and other audiovisual works for purposes of criticism and comment.

[111] The current regulatory language for these exemptions is set forth in 37 C.F.R. § 201.40(4)-(7). By way of example, a portion of the language allowing for the circumvention of the CSS protection system on DVDs provides as follows:

> (4) Motion pictures, as defined in 17 U.S.C. 101, on DVDs that are lawfully made and acquired and that are protected by the Content Scrambling System, where the person engaging in circumvention believes and has reasonable grounds for believing that circumvention is necessary because reasonably available alternatives, such as noncircumventing methods or using screen capture software as provided for in alternative exemptions, are not able to produce the level of high-quality content required to achieve the desired criticism or comment on such motion pictures, and where circumvention is undertaken solely in order to make use of short portions of the motion pictures for the purpose of criticism or comment in the following instances:
>
> (i) In noncommercial videos;
>
> (ii) In documentary films;
>
> (iii) In nonfiction multimedia e-books offering film analysis; and
>
> (iv) For educational purposes in film studies or other courses requiring close analysis of film and media excerpts, by college and university faculty, college and university students, and kindergarten through twelfth grade educators.
>
> For purposes of this exemption, "noncommercial videos" includes videos created pursuant to a paid commission, provided that the commissioning entity's use is noncommercial.

Class 1 concerns educational uses at colleges and universities; for example, this class would allow film studies professors to circumvent DVDs in order to use motion picture clips in class lectures. Petitioners for this class were Professor Peter Decherney, the College Art Association, the International Communication Association, and the Society for Cinema and Media Studies (collectively, "Joint Educators").[112] Short-form comments supporting this exemption were filed by Professor Jeremy Sheff, Music Library Association ("MLA"), the Free Software Foundation ("FSF"), and over 1500 other individuals.[113]

> The NPRM described Proposed Class 2 as follows:
>
> Proposed Class 2: This proposed class would allow kindergarten through twelfth-grade educators and students to circumvent access controls on lawfully made and acquired motion pictures and other audiovisual works for educational purposes.

Class 2 concerns educational uses in kindergarten through twelfth grades; for example, this class would allow a high school teacher to circumvent DVDs of various adaptations of Shakespeare's works in order to create a compilation of clips demonstrating the lasting influence of these works. Petitions for Proposed Class 2 were submitted by Professor Renee Hobbs[114] and the Library Copyright Alliance ("LCA").[115] During the public comment phase, Hobbs' comments were co-signed by the American Library Association ("ALA"), Professor Frances Jacobson Harris, Professor Sherri Hope Culver and Michelle Ciulla Lipkin of the National Association for Media Literacy Education

[112] The petition was submitted on their behalf, and petitioners were also represented throughout the rulemaking proceeding, by the Glushko-Samuelson Intellectual Property Law Clinic at Washington College of Law, American University. Joint Educators' proposed regulatory language reads as follows: "Audiovisual works embodied in physical media (such as DVDs and Blu-Ray Discs) or obtained online (such as through online distribution services and streaming media) that are lawfully made and acquired and that are protected by various technological protection measures, where the circumvention is accomplished by college and university students or faculty (including teaching and research assistants) . . . for the purpose of criticism or comment." Joint Educators Pet. at 1.

[113] Sheff Supp.; MLA Class 1 Supp.; FSF Class 1 Supp.; Digital Right to Repair Class 1 Supp. (1501 individuals).

[114] Hobbs proposed that the Register recommend "an exemption that enables educators and students in grades K-12 . . . to 'rip' encrypted or copy-protected lawfully accessed audiovisual works used for educational purposes." Hobbs Pet. at 1.

[115] LCA requested "renewal of the exemption granted in the 2012 rulemaking for motion picture excerpts. The exemption should be broadened to apply to all storage media, including Blu-Ray. Further, the exemption for educational purposes should be expanded to apply to students in kindergarten through twelfth grade. LCA also seeks simplification of the exemption so that it could be readily understood by the authors, filmmakers, students, and educators it is intended to benefit." LCA Motion Picture Excerpts Pet. at 1.

("NAMLE"), and Media Literacy Now, Inc.[116] In addition, MLA and FSF filed short-form comments in support of the exemption.[117]

> The NPRM described Proposed Class 3 as follows:
>
> Proposed Class 3: This proposed class would allow students and faculty participating in massive online open courses ("MOOCs") to circumvent access controls on lawfully made and acquired motion pictures and other audiovisual works for purposes of criticism and comment.

Class 3 concerns educational uses in MOOCs; for example, this class would allow a professor preparing an online lecture about the evolution of Chinese society to circumvent access controls in order to incorporate video clips documenting Chinese history and geography. Joint Educators proposed Class 3.[118] In addition, MLA and FSF filed short-form comments in support of the exemption.[119]

> The NPRM described Proposed Class 4 as follows:
>
> Proposed Class 4: This proposed class would allow educators and learners in libraries, museums and nonprofit organizations to circumvent access controls on lawfully made and acquired motion pictures and other audiovisual works for educational purposes.

Class 4 concerns educational uses in libraries, museums, and nonprofit organizations; for example, this class would allow educators in a community center adult education program to circumvent access controls in order to create video clips for purposes of discussing the portrayal of African-American women in a popular television show. Professor Hobbs proposed Class 4.[120] During the public comment phase, Hobbs' comments were co-signed by LCA, NAMLE, Philly CAM: Philadelphia Public Access

[116] Hobbs Class 2 Supp. at 1. Although ALA is a member of LCA, LCA did not separately join Hobbs' written submissions.

[117] MLA Class 2 Supp.; FSF Class 2 Supp.

[118] Joint Educators, in relevant part, proposed the following regulatory language: "Audiovisual works embodied in physical media (such as DVDs and Blu-Ray Discs) or obtained online (such as through online distribution services and streaming media) that are lawfully made and acquired and that are protected by various technological protection measures, where the circumvention is accomplished by . . . students and faculty participating in Massive Open Online Courses (MOOCs) for the purpose of criticism or comment." Joint Educators Pet. at 1.

[119] MLA Class 3 Supp.; FSF Class 3 Supp.

[120] Hobbs proposed that the Register extend the existing exemption to "educators and learners in libraries, museum and nonprofit organizations." Hobbs Pet. at 1.

Center, Media Literacy Now, Inc., and The LAMP NYC.[121] In addition, MLA and FSF filed short-form comments in support of the exemption.[122]

> The NPRM described Proposed Class 5 as follows:
>
> Proposed Class 5: This proposed class would allow circumvention of access controls on lawfully made and acquired motion pictures used in connection with multimedia e-book authorship.

Class 5 concerns derivative uses of motion picture excerpts in e-books; for example, this class would allow a sound editor and e-book author to circumvent DVDs or Blu-ray discs in order to incorporate brief film excerpts in an e-book entitled *Listening to Movies*. Class 5 was jointly proposed by Authors Alliance and Bobette Buster.[123] During the public comment phase, Authors Alliance and Bobette Buster filed joint comments with the American Association of University Professors, the Society for Cinema and Media Studies, the University Film and Video Association, and Mark Berger (collectively, "Authors Alliance").[124] In addition, short-form comments supporting the exemption were filed by MLA, FSF, and over 1400 individuals.[125]

> The NPRM described Proposed Class 6 as follows:
>
> Proposed Class 6: This proposed class would allow circumvention of access controls on lawfully made and acquired motion pictures for filmmaking purposes.

Class 6 concerns derivative uses of motion picture excerpts in filmmaking; for example, this class would allow filmmakers to circumvent access controls on material streamed online in order to incorporate excerpts of news footage into documentaries. A petition for Class 6 was jointly filed by International Documentary Association, Film Independent, Kartemquin Educational Films, Inc., and National Alliance for Media Arts and Culture (collectively, "Joint Filmmakers").[126] A long-form comment in support of

[121] Hobbs Class 4 Supp. at 1.

[122] MLA Class 4 Supp.; FSF Class 4 Supp.

[123] The petition was submitted on their behalf, and petitioners were also represented throughout the rulemaking proceeding, by the UCI Intellectual Property Arts and Technology Clinic at University of California, Irvine ("UCI") and the Samuelson-Glushko Technology Law & Policy Clinic at Colorado Law. Petitioners jointly proposed an exemption "that permits authors of multimedia e-books to circumvent Content Scramble System ('CSS') on DVDs, Advanced Access Content System ('AACS') on Blu-ray discs, and encryption and authentication protocols on digitally transmitted video in order to make fair use of motion picture content in their e-books." Authors Alliance Pet. at 2.

[124] Authors Alliance Class 5 Supp. at 1.

[125] MLA Class 5 Supp.; FSF Class 5 Supp.; Digital Right to Repair Class 5 Supp. (1408 individuals).

[126] The petition was submitted on their behalf, and petitioners were also represented throughout the rulemaking proceeding, by UCI and Donaldson & Callif, LLP. Specifically, Joint Filmmakers proposed an exemption to allow circumvention of TPMs for "filmmakers who seek to make fair use in their filmmaking

the exemption was received from New Media Rights ("NMR").[127] In addition, short-form comments supporting the exemption were filed by FSF and over 1500 individuals.[128]

The NPRM described Proposed Class 7 as follows:

> Proposed Class 7: This proposed class would allow circumvention of access controls on lawfully made and acquired audiovisual works for the sole purpose of extracting clips for inclusion in noncommercial videos that do not infringe copyright.

Class 7 concerns derivative uses of motion picture excerpts in noncommercial videos, including remix videos; for example, this class would allow a fan of *James Bond* films to circumvent access controls on DVDs of these films in order to incorporate brief excerpts into a video commenting on the portrayal of female characters in those films. Petitioners of Class 7 were the Electronic Frontier Foundation ("EFF") and the Organization for Transformative Works ("OTW") (collectively, "EFF/OTW").[129] Long-form comments supporting the exemption were filed by NMR.[130] Short-form comments providing specific examples of noncommercial videos were filed by the National Congress of American Indians ("NCAI") and the USC Norman Lear Center.[131] In addition, short-form comments expressing general support for the exemption were filed by MLA, FSF, and over 1500 individuals.[132]

Because these proposed audiovisual exemptions involve many overlapping factual and legal issues relating to the use of clips from motion pictures or other audiovisual works, Proposed Classes 1 through 7 are addressed as a group.

---

of copyrighted motion pictures protected by TPMs on DVDs, Blu-ray discs, and digitally transmitted video." Joint Filmmakers Pet. at 2.

[127] NMR Class 6 Supp.

[128] FSF Class 6 Supp.; Digital Right to Repair Class 6 Supp. (1565 individuals).

[129] EFF/OTW submitted two separate petitions, one relating to DVD and Blu-ray discs and one relating to digitally transmitted material, which the Office consolidated into a single class. The respective petitions sought exemptions for "[a]udiovisual works on DVDs and Blu-Ray discs that are lawfully made and acquired and that are protected by Digital Rights Management schemes, where circumvention is undertaken for the sole purpose of extracting clips for inclusion in noncommercial videos that do not infringe copyright" and "[a]udiovisual works that are lawfully made and acquired via online distribution services, where circumvention is undertaken solely for the purpose of extracting clips for inclusion in noncommercial videos that do not infringe copyright." EFF/OTW Disc Remix Pet. at 1; EFF/OTW Online Remix Pet. at 1.

[130] NMR Class 7 Supp.

[131] *See* NCAI Supp.; USC Norman Lear Center Supp.

[132] MLA Class 7 Supp.; FSF Class 7 Supp.; Digital Right to Repair Class 7 Supp. (1574 individuals).

a. Background

Proposed Classes 1 through 7 share the desire to circumvent TPMs employed on DVDs, Blu-ray discs, and/or by various online streaming services. The proponents generally contend that they need to circumvent controls protecting each technology in order to access unique and/or higher-quality material available on the platform in question.

The vast majority of DVDs use the Content Scramble System ("CSS") to encrypt audiovisual works on DVDs using a fixed set of decryption keys, and the Copyright Office and courts have found that CSS is an "access control" within the meaning of section 1201(a)(1).[133] The CSS key was decoded in 1999, and decryption software is now available on the internet, including the programs MactheRipper, DVDDecrypter, and Handbrake.[134]

Blu-ray discs are protected primarily by the Advanced Access Content System ("AACS"), which allows vendors to revoke compromised keys and distribute new keys.[135] In 2012, the Register recognized AACS as a TPM subject to the DMCA.[136] Proponents, including EFF/OTW, attest that Blu-ray circumvention tools are also easily available, including DVDFab and MakeMKV.[137] Another TPM, called BD+, protects some Blu-ray discs.[138]

According to Joint Filmmakers, access controls used by online streaming services vary widely, and some services, such as Vimeo's online video sharing service, use no encryption or other access control technologies.[139] But other services, such as Netflix, protect streamed content through encryption and other protocols such as Microsoft Silverlight, Adobe Flash, or Apple's proprietary FairPlay scheme.[140] Commenters generally agreed that the relevant TPMs for online media are in a "state of flux," as Silverlight and Flash are scheduled to be discontinued and HTML5, a newer web standard that is being widely adopted, has encryption capabilities under development.[141] Accordingly, while Joint Filmmakers provided information on current TPMs for online

---

[133] *See* EFF/OTW Supp. at 2; Joint Filmmakers Supp. at 2; *see also* 2012 Recommendation at 126; *DVD Copy Control Ass'n, Inc. v. Bunner*, 116 Cal. App. 4th 241, 255 (Cal. Ct. App. 2004).

[134] Joint Filmmakers Supp. at 2; EFF/OTW Supp. at 2 & n.5. The Register notes that distribution of these tools would appear to run afoul of the DMCA's anti-trafficking provision in section 1201(a)(2), and reiterates that any exemption granted here would not affect a traffickers' liability under that provision. *See* 17 U.S.C. § 1201(a)(2).

[135] Joint Filmmakers Supp. at 3.

[136] 2012 Recommendation at 126.

[137] *See, e.g.*, EFF/OTW Supp. at 2 & n.5.

[138] *Id.* at 2.

[139] Joint Filmmakers Supp. at 3, App. J (Letter from Alex Podobas).

[140] *Id.*; EFF/OTW Supp. at 2

[141] Joint Filmmakers Supp. at 3, App. J at 2-3 (Letter from Alex Podobas).

streaming services, they request that an exemption not be limited to a subset of streaming technologies to avoid becoming "obsolete long before the exemption expire[s]."[142]

In addition to seeking to circumvent the same types of access controls, some of the proposals share other commonalities. A number of the proposals seek to access content on audiovisual works that are not motion pictures, such as video games. Notably, many of the proposals seek to circumvent access controls to obtain motion picture clips for broader purposes than covered by previous exemptions, such as use of more than "short portions" of motion picture excerpts, or use for all "fair uses" rather than for purposes of criticism or comment. Other proposals were focused on expanding the category of potential users of an exemption, such as to fictional filmmakers or uses by museums, libraries and nonprofits, or students and faculty participating in MOOCs. The specific proposals are described below.

i. Proposed Class 1: Colleges and Universities

Joint Educators seek an exemption similar to ones that were adopted in the 2010 and 2012 rulemakings.[143] The proposal diverges from the exemption adopted in 2012 in a few respects, however. First, the petition requests that any exemption include the circumvention of AACS-protected Blu-ray discs, a proposal that the Register declined to recommend in 2012.[144] Joint Educators maintain that in the past three years, user expectations for video delivery technology have advanced and high-definition ("HD") images, such as those provided by Blu-ray discs, have become standard.[145] Second, the petition seeks an exemption for uses for "educational purposes," as opposed to the more limited language of the 2012 exemption for uses "in film studies or other courses requiring close analysis of film and media excerpts." This is a variant upon Joint Educators' request in 2012, when, based upon the record, the Register declined to recommend that the exemption apply to "students across all disciplines of study."[146] Third, the petition is not limited to uses of "short portions" of audiovisual material, a limitation the Register found critical in 2012.[147] Finally, the petition defines the class of works as "audiovisual works," a proposal that the Register declined to recommend in 2012 based on the record—which was focused on motion picture uses—instead limiting her recommendation to "motion pictures."[148]

---

[142] Joint Filmmakers Supp. at 4, App. J at 4 (Letter from Alex Podobas).

[143] 2012 Final Rule, 77 Fed. Reg. at 65,278-79; 2010 Final Rule, 75 Fed. Reg. at 43,839.

[144] 2012 Recommendation at 135.

[145] Joint Educators Class 1 Supp. at 13-15. (In supporting comments, the petitioning Joint Educators were joined by Michael X. Delli Carpini, Professor and Dean, Annenberg School for Communication, American Association of University Professors, and LCA.)

[146] 2012 Recommendation at 138-39.

[147] *Id.* at 138.

[148] *Id.* at 125-26.

ii. Proposed Class 2: Primary and Secondary Schools (K-12)

The proposals for an exemption to facilitate educational uses of motion picture excerpts at the kindergarten through twelfth-grade levels diverge from the exemption adopted in 2012 in a few respects.[149] First, proponents request that the exemption extend to student uses for each of the requested technologies, whereas the 2012 exemption was limited to student use of screen-capture technologies.[150] Second, Hobbs' proposal seeks an exemption for uses for "educational purposes," as opposed to for uses "in film studies or other courses requiring close analysis of film and media excerpts."[151] Third, as in Proposed Class 1, proponents request that any exemption include the circumvention of AACS-protected Blu-ray discs, which the Register declined to recommend in 2012.[152] Fourth, the Hobbs proposal as written could encompass more than "motion pictures" since the language used is "audiovisual works."[153] For its part, LCA suggests that the wording of the current exemption should be simplified for the benefit of its users.[154]

iii. Proposed Class 3: Massive Open Online Courses (MOOCs)

Joint Educators' petition requests that any exemption for college and university faculty and staff include those participating in MOOCs, or online distance education courses offered on a broad scale, which have gained popularity since the last triennial rulemaking.[155] According to the petition, "MOOCs typically consist of pre-recorded lectures that may be illustrated, as appropriate, with short clips and still images from audiovisual works."[156] In its NPRM, the Office encouraged commenters to address how the Office might define "MOOC" for the purpose of the proposed exemption, "including but not limited to (a) courses offered with free and open content versus courses that require course materials to be licensed by users, (b) courses requiring registration and/or identity verification versus courses without such requirements, (c) courses offered for

[149] *See* 37 C.F.R. § 201.40(b)(4)-(7); 2012 Final Rule, 77 Fed. Reg. at 65,266-70.

[150] 2012 Recommendation at 140-42.

[151] *See id.* at 138-42.

[152] Hobbs Pet. at 2; 2012 Recommendation at 135.

[153] The Copyright Act defines audiovisual works as "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." 17 U.S.C. § 101. "Motion pictures" are defined in the Copyright Act as "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." *Id.* Under the Copyright Act, then, the category of audiovisual works is broader than motion pictures, but the term "motion pictures" includes non-feature film material such as television shows, commercials, and videos.

[154] LCA Motion Picture Excerpts Pet. at 1.

[155] Joint Educators Pet. at 1.

[156] *Id.* at 4.

free versus paid courses, and (d) whether the provider is a nonprofit or for-profit entity."[157]

In addition to expanding the group of potential users of this exemption to participants in MOOCs, the proposal seeks the same expansions from the 2012 Recommendation as Class 1—namely, to include the ability to circumvent Blu-ray discs, to remove the limitation to "short portions" of motion picture excerpts, and to broaden the class to cover all "audiovisual works" for all "educational purposes."

iv. Proposed Class 4: Educational Programs Operated by Museums, Libraries or Nonprofits

The Hobbs petition for Proposed Class 4 requests an exemption to apply to "educators and learners in libraries, museum and nonprofit organizations."[158] This is the first time an exemption covering such persons has been requested. According to Hobbs, there are over 123,000 libraries and 3000 public, educational, and government media access centers in the United States.[159] The petition states that "[s]ome of the most important and innovative work in media literacy education is occurring in libraries, museums and afterschool programming, supported by non-profit organizations and charitable foundations."[160]

Efforts were made during the rulemaking to ensure this proposal was adequately defined. In its NPRM, the Office encouraged commenters to address, among other issues, who should be included in the proposed categories of "educators" and "learners," whether the exemption should treat prepared presentations by museums, libraries and nonprofits differently than hands-on learning projects, and whether the exemption should be limited to use and display within physical spaces as opposed to online uses.[161] In reply comments, Professor Hobbs submitted that if necessary, an exemption could be limited to "digital and media literacy instructional practices in informal learning contexts."[162] At the public hearing, Professor Hobbs further indicated that any exemption could properly exclude "exhibition" uses by museums and other institutions.[163]

In addition to expanding the group of potential users that might benefit from such an exemption, the proposal seeks the same expansions from the 2012 Recommendation as the Hobbs proposal for Class 2—namely, an exemption for "audiovisual works" as opposed to "motion pictures," and for "educational uses," as opposed to studies requiring

[157] NPRM, 79 Fed. Reg. at 73,861.

[158] Hobbs Pet. at 1.

[159] Hobbs Class 4 Reply at 2.

[160] Hobbs Pet. at 2.

[161] NPRM, 79 Fed. Reg. at 73,861.

[162] Hobbs Class 4 Reply at 8.

[163] Tr. at 237:09-16 (May 27, 2015) (Hobbs).

close analysis of film and media excerpts, as well as the ability to circumvent Blu-ray discs.

v. Proposed Class 5: Multimedia E-Books

Authors Alliance generally seeks renewal of a previously granted exemption permitting circumvention of TPMs for purposes of facilitating uses of motion picture excerpts in nonfiction multimedia e-books offering film analysis.[164] The petition requests a few modifications to the previously granted exemption. First, the petition requests that any exemption include the circumvention of AACS-protected Blu-ray discs, a proposal that the Register declined to recommend in 2012.[165] Second, the petition seeks an exemption in order to "make fair use of motion picture content" in any genre of multimedia e-book, as opposed to the more limited language of the 2012 exemption for uses "in nonfiction multimedia e-books offering film analysis."[166] Third, the petition is not limited to uses of "short portions" of audiovisual material, a limitation the Register found critical in 2012.[167] Finally, although the initial proposal was limited to "motion pictures" at the public hearing, Authors Alliance suggested that video game excerpts should be included within this exemption.[168]

vi. Proposed Class 6: Filmmaking Uses

Joint Filmmakers seek adoption of a revised version of the previously granted exemption to permit circumvention of TPMs on DVDs, Blu-ray discs, and videos acquired via online distribution services, for purposes of facilitating uses of motion picture excerpts in documentary films.[169] Prior rulemakings have granted exemptions for documentary filmmaking, limited to uses of short clips, and did not extend to Blu-ray discs.[170] In limiting her Recommendation in 2012 to uses in documentary, as opposed to narrative (or fictional) filmmaking, the Register noted that the record in that rulemaking proceeding did "not allow the Register to reach a satisfying determination as to the nature of the fictional filmmakers' proposed uses, the amount of the underlying works fictional filmmakers generally seek to use, or whether or how such uses might affect the market for the original works."[171] In this proceeding, proponents again seek a broader exemption that would cover all types of films, including narrative (or fictional) films.[172] According to Joint Filmmakers, "makers of narrative films with fictional content rely on

[164] Authors Alliance Pet. at 2.

[165] 2012 Recommendation at 135.

[166] Authors Alliance Pet. at 2.

[167] 2012 Recommendation at 138.

[168] Tr. at 51:12-53:15 (May 28, 2015) (Lerner, Authors Alliance/Buster).

[169] Joint Filmmakers Pet. at 1.

[170] *See, e.g.*, 37 C.F.R. § 201.40(b)(4)-(7); 2012 Recommendation at 138-142.

[171] 2012 Recommendation at 130.

[172] Joint Filmmakers Supp. at 2.

fair use and the DMCA is causing harm to that use; the exemption must be modified to account for all filmmakers."[173]

vii. Proposed Class 7: Noncommercial Videos

According to EFF/OTW, the past few years have seen an explosion of noncommercial videos, including "remix" videos, because of easy-to-use and inexpensive or free video editing tools and hosting services.[174] EFF/OTW characterize these videos as "original, primarily noncommercial videos that include clips taken from works released on DVD and Blu-ray [or from authorized online distribution sources]."[175] EFF/OTW claim that 2.6% of U.S. internet users have created remix videos, and "between 2,000 and 6,000 original fair use videos that include clips from DRM-protected film or television sources are likely being uploaded to YouTube *each day.*"[176] EFF/OTW ask for a renewal of the existing exemption, which covers "noncommercial videos," and, as discussed below, resist opponents' suggestion to narrow the proposed exemption to "remix videos" specifically.[177] The record reflects that some purportedly noncommercial videos submitted in this category—for example, the *Take It Away* video commenting upon the Washington Redskins' logo discussed below—might not constitute what are commonly understood as remixes.

The current proposal represents an expansion upon the 2012 rulemaking. First, the petition requests that any exemption include the circumvention of AACS-protected Blu-ray discs, a proposal that the Register declined to recommend in 2012.[178] Second, EFF/OTW oppose limiting the exemption to uses "for purposes of criticism, comment, or education," instead of simply "noninfringing" or "fair" uses.[179] EFF/OTW additionally request that the recommendation include interpretative guidance in relation to phrases like "short clips," "motion pictures," or "primarily noncommercial," but does not oppose maintaining such language, used in 2012, in a new exemption.[180]

---

[173] *Id.*

[174] EFF/OTW Supp. at 3.

[175] EFF/OTW Disc Remix Pet. at 2; EFF/OTW Online Remix Pet. at 3*; see also* EFF/OTW Online Remix Pet. at 2 (defining "fanworks" as "new, noncommercial creative works based on existing media").

[176] EFF/OTW Supp. at 3 (emphasis in original).

[177] *See* EFF/OTW Class 7 Post-Hearing Resp. (very narrow exemptions may lack clarity and exclude protected uses); Band/Butler/Decherney Class 7 Post-Hearing Resp.

[178] 2012 Recommendation at 135.

[179] EFF/OTW Supp. at 22.

[180] *See id.* at 22-24; Tr. at 309:22-311:12 (May 28, 2015) (McSherry, EFF; Tushnet, OTW; Charlesworth, USCO; Smith, USCO). For example, EFF/OTW recommended that any regulation make clear to "laypeople that 'motion pictures' includes television and streaming video," but did not seek to expand the previously granted exemption to all "audiovisual works." EFF/OTW Supp. at 22.

b. Asserted Noninfringing Uses

i. Proposed Class 1: Colleges and Universities

Joint Educators claim that the proposed uses of motion picture excerpts by college and university educators and students are non-infringing as analyzed under the four statutory fair use factors.[181] According to Joint Educators: (1) the first factor favors the requested exemption because the proposed class is strictly educational and the repurposing of audiovisual works for criticism or commentary is transformative; (2) the second factor, the nature of the underlying copyrighted work, is of limited use since the requested exemption would apply to a range of works ranging from fictional to factual, but all uses are likely to be transformative; (3) the third factor favors the requested exemption because the amount taken is limited to excerpts incorporated directly into lectures or presentations; and (4) the fourth factor favors the requested exemption because educational uses are not a market substitute for the underlying work but could spur libraries to purchase additional copyrighted works.[182] Because teaching, criticism, and comment are enumerated as favored uses under section 107 and because the proposed uses are alleged to be transformative, Joint Educators argue that users are highly likely to be engaging in fair use.[183]

Joint Educators contend that the noninfringing nature of these uses extends across disciplines, and the record demonstrates that the existing exemption was used in courses spanning art, biology, communication, English, film, foreign language and literature, law and music studies.[184] In support of this position, for example, law professor Jeremy Sheff documented his use of embedded, high-quality clips obtained from a circumvented DVD as a teaching tool in his property law courses.[185]

ii. Proposed Class 2: Primary and Secondary Schools (K-12)

The proponents assert that the proposed uses of works in pre-college settings, including uses requiring access to high-resolution excerpts, are lawful fair uses under section 107. First, the proposed uses are for nonprofit educational purposes. Hobbs submitted multiple examples of educators using film clips as teaching tools in connection with media literacy, history, literature, and film theory,[186] and of students using excerpts in connection with National History Day[187] and digital remix projects.[188] Hobbs also

[181] Joint Educators Class 1 Supp. at 4-6.

[182] *Id.*

[183] *Id.* at 4-5.

[184] *Id.* at 7.

[185] Sheff Supp. at 1.

[186] Hobbs Class 2 Supp. at 4-5 (discussing comparison of the film *Chicago* with the book *The Great Gatsby,* analysis of Shakespearean works, study of usage of tones in video journalism, study of *Citizen Kane,* and study of film theory in high school English classes).

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

asserts that students often create "transformative content using motion picture excerpts."[189]

Second, Hobbs argues that the nature of the copyrighted work varies depending upon material, but may be creative and expressive. Third, Hobbs contends it is inappropriate to limit an exemption to "short" or "brief" excerpts of works, and that use of long excerpts can also be a fair use.[190] Other proponents, however, accept the limitation in the existing exemption to uses of "short clips" and argue that, based on that limitation, the third fair use factor weighs in favor of fair use.[191] Finally, as to the fourth factor, Hobbs asserts that the uses are transformative and that an exemption would have no effect on the market for copyrighted works.[192]

iii. Proposed Class 3: Massive Open Online Courses (MOOCs)

Essentially, Joint Educators argue that students and faculty participating in online distance learning are encumbered by the same restrictions that would hinder traditional educational contexts if not for the current exemption.[193] Joint Educators explain that the prevalence of MOOCs has grown dramatically in the past three years, with up to 18 million students participating in over 2,400 courses in 2014.[194] According to them, "[m]ost MOOCs are taught by the same college and university professors that teach those courses at [traditional] institutions across the country."[195] Joint Educators explain, however, that not all MOOCs require registration, courses may be made available without charge, and two of the four most popular platforms for MOOCs—Coursera and Udacity—are for-profit entities.[196]

In claiming that the courses available from MOOCs are the "online equivalent of core traditional educational uses," Joint Educators argue that the proposed uses are substantially likely to be fair uses under section 107 for the same reasons as uses in a traditional classroom.[197] Considering the first factor, they assert that the purpose and

---

[188] *Id.* at 3; Hobbs Class 2 Reply at 4.

[189] Hobbs Class 2 Supp. at 3.

[190] Hobbs Class 2 Reply at 5 (citing *Cambridge Univ. Press v. Patton*, 769 F.3d 1232 (11th Cir. 2014)).

[191] MLA Class 2 Supp. at 1; FSF Class 2 Supp. at 1.

[192] Hobbs Class 2 Supp. at 3, 9; Hobbs Class 2 Reply at 8-9.

[193] Joint Educators Class 3 Supp. at 2. (In supporting comments, the petitioning Joint Educators were joined by Michael X. Delli Carpini, Professor and Dean, Annenberg School for Communication, American Association of University Professors, and the LCA.)

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

[195] *Id.* at 21.

[196] *Id.* at 5-6; Tr. at 105:14-17 (May 27, 2015) (Butler, Joint Educators). Some MOOCs charge for completion certificates. Tr. at 106:19-107:03 (May 27, 2015) (Decherney, Joint Educators). The leading non-profit platforms are Coursera, edX, the Khan Academy, and Udacity. Joint Educators Class 3 Supp. at 6.

[197] Joint Educators Class 3 Supp. at 8, 13-15.

character of the use is a favored educational use. According to Joint Educators, the "vast majority" of MOOCs are taught by college and university professors, and the leading providers are "either partnered with or owned by colleges or universities."[198] As examples, Joint Educators reference a series of courses on China's past, present, and future titled *ChinaX* offered by Harvard that could make use of motion picture clips to "highlight the beauty of the country and provide enrolled students with a sense of its culture," as well as an upcoming course titled *The Hollywood Film Industry* planned by Professor Decherney of University of Pennsylvania, which is modeled after his face-to-face lectures in cinema studies.[199]

Joint Educators also point out that for-profit uses are not necessarily precluded from being fair uses, noting that the Supreme Court has stated "nearly all of the illustrative uses listed in the preamble paragraph of § 107, including news reporting, comment, criticism, teaching, scholarship, and research . . . are generally conducted for profit in this country," and that the House Report on the 1976 Copyright Act explicitly warned against incorporating a not-for-profit limitation into the definition of educational uses of copyrighted works.[200] The record, however, does not appear to contain examples of proposed uses in connection with MOOCs operated on a for-profit basis. Instead, the examples in the record are all of courses offered by a nonprofit accredited educational institution (*e.g.*, University of Pennsylvania or Harvard University) that are accessible from a platform (*e.g.*, edX or Coursera) that may or may not be a for-profit company.[201]

As with other proposed educational uses, Joint Educators note that the second fair use factor, the nature of the copyrighted works, will vary, though based on the examples they provide, it can be assumed that the uses will include creative and expressive works. As for the third factor, because MOOC video lectures are typically only seven to ten minutes long, Joint Educators assert that the amount of the copyrighted works used would be limited to brief material essential for the pedagogical purpose.[202] Finally, as to the fourth factor, Joint Educators claim that the transformative nature of the uses eliminates any risk of market harm.[203]

Joint Educators also addressed the NPRM's query whether section 110(2) of the Copyright Act (often referred to as the "TEACH Act") might impact this proposed class.[204] Enacted in 2002, the TEACH Act provides an exception in copyright law for

---

[198] Joint Educators Class 3 Reply at 9.

[199] Joint Educators Class 3 Supp. at 12-13.

[200] Joint Educators Class 3 Reply at 6-7 (quoting *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 584 (1994) and H.R. REP. NO. 94-1476, at 66 (1976)).

[201] The record indicates that edX is operated on a nonprofit basis and its competitor Coursera is operated on a for-profit basis.

[202] Joint Educators Class 3 Supp. at 9, 15.

[203] Joint Educators Class 3 Reply at 7-8.

[204] NPRM, 79 Fed. Reg. at 73,861.

certain uses of copyrighted works by nonprofit educators in distance education.[205] The Act outlines a number of requirements in order to make use of this section, many of which are potentially relevant to the proposed class. First, the transmitter of the copyrighted works must be "a governmental body or an accredited nonprofit educational institution."[206] Second, the use must be made at the direction of an instructor teaching a class session as "a regular part of the systematic mediated instructional activities" and in an amount "comparable to that which is typically displayed in the course of a live classroom session."[207] Third, the reception of the transmission must be limited, to the extent feasible, to students officially enrolled in the course.[208] Fourth, the transmitting educational institution must institute policies and provide notice regarding copyright protection to students, faculty, and relevant staff members.[209] Finally, the transmitting body must apply technological measures that limit the retention and unauthorized further dissemination of the work in accessible form.[210]

Joint Educators assert that they do not find the TEACH Act to be especially useful to their petition or analysis.[211] They note that Congress recognized a value in allowing "reasonable and limited portions" of audiovisual works for distance learning, and rely on this fact to suggest that the proposed uses are "favored" in copyright law.[212] But they also suggest that many MOOC offerings would be prohibited from qualifying under section 110(2) by the requirements that the uses be made in connection with a "class session" for enrolled students, and as part of "systemic mediated instructional activities" offered by "an accredited, non-profit institution."[213] Because the meanings of these terms are relatively untested by the courts, Joint Educators suggest that they may discourage potential users.[214] Further, Joint Educators claim that section 110(2)'s requirement that

---

[205] 17 U.S.C. § 110(2); *see also* U.S. COPYRIGHT OFFICE, REPORT ON COPYRIGHT AND DIGITAL DISTANCE EDUCATION (1999), *available at* http://www.copyright.gov/reports/de_rprt.pdf.

[206] 17 U.S.C. § 110(2).

[207] *Id.*

[208] *Id.*

[209] *Id.*

[210] *Id.*

[211] Joint Educators Class 3 Supp. at 16.

[212] Joint Educators Class 3 Reply at 5; Tr. at 101:09-12 (May 27, 2015) (Band, LCA) (noting that "it would be helpful to use [110(2)] as a starting point").

[213] Joint Educators Class 3 Supp. at 16; *see also* Tr. at 112:06-114:06 (May 27, 2015) (Decherney, Joint Educators; Charlesworth, USCO) (discussing proponents' view that MOOCs offered by University of Pennsylvania would not qualify under section 110(2) because, although they are password-protected and limited to registered users, the videos are not encrypted and the MOOC may be "closer to the next generation of textbook" than a lecture); Band/Butler/Decherney Class 3 Post-Hearing Resp. at 2-4 (stating that half of Coursera's video traffic is via download in developing countries, and one-third of its traffic is via download in developed countries).

[214] *See* Band/Butler/Decherney Class 3 Post-Hearing Resp. at 1, 4; Tr. at 101:14-17 (May 27, 2015) (Band, LCA).

online courses implement TPMs would be "an unwelcome and unnatural fit" for providers of popular MOOC platforms such as Coursera, EdX, FutureLearn, and the Canvas Network.[215]

iv. Proposed Class 4: Educational Programs Operated by Museums, Libraries or Nonprofits

Proponent Hobbs argues that uses of motion picture excerpts in digital and media literacy programs offered by museums, libraries and nonprofits are "highly likely to be fair uses" because these "innovative educational practices" allow users to critically analyze and create media.[216] Hobbs states that "teachers and learners in informal settings need to use film clips for a wide range of teaching and learning purposes characterized broadly as educational use."[217] Hobbs provides examples of student-created video poetry essays in connection with a GED-conferring program, and an adult education program analyzing the portrayal of African-American women in the television series *Orange is the New Black*.[218] Hobbs also references various after-school programs, but does not specify how these programs seek to use motion picture excerpts obtained by circumventing TPMs. Hobbs urges the Register to treat learning in these "informal" settings as on par with exemptions for K-12 teachers, or university students in media studies classes, arguing that to distinguish among these settings would perpetuate educational inequities.[219]

Although the record is rather sparse regarding the specifics of the proposed uses, Hobbs contends generally that these types of uses are likely to be fair under the statutory factors. First, Hobbs asserts that these uses qualify as fair uses because their purpose is to facilitate criticism, comment, learning, and teaching.[220] Second, Hobbs claims that the nature of the work, including "entertainment, informational, and other forms of contemporary and classic film and video content" is relevant to learners today, though she does not explain how the second factor favors an exemption.[221] Third, Hobbs suggests a specific numerical time limit for "short" or "brief" clips is not required by the law.[222] Fourth, Hobbs states that the proposed uses would not impair the market for the underlying copyrighted works.[223]

---

[215] Band/Butler/Decherney Class 3 Post-Hearing Resp. at 2.

[216] Hobbs Class 4 Reply at 3-4.

[217] Hobbs Class 4 Supp. at 3.

[218] *See id.*at 4; Hobbs Class 4 Reply at 4, 8; Tr. at 231:09-232:08, 234:11-235:25, 258:14-259:08 (May 27, 2015) (Hobbs).

[219] Hobbs Class 4 Reply at 4.

[220] Hobbs Class 4 Supp. at 4-5.

[221] *Id.*at 4.

[222] Hobbs Class 4 Reply at 6 (citing *Cambridge*, 769 F.3d 1232).

[223] Hobbs Class 4 Supp. at 4-5.

v. Proposed Class 5: Multimedia E-Books

Authors Alliance argues that the use of excerpts of motion picture clips in multimedia e-books, especially ones intended for educational purposes, presents "a strong case for fair use."[224] Proponents do not offer a full analysis of their proposed uses under the four fair use factors. They do, however, describe numerous examples of actual or prospective uses of motion picture excerpts in multimedia e-books for purposes of film criticism or analysis.[225] For example, proponent Berger is an Academy-Award winning sound editor who wishes to make an e-book entitled *Listening to Movies* that includes film clips to analyze how sound relates to a film's moving images.[226] Similarly, proponent Buster, a professor in cinema studies, plans to publish an e-book series entitled *Deconstructing Master Filmmakers* that would incorporate and analyze short excerpts from feature films.[227] Authors Alliance also briefly addresses the third factor, amount and substantiality of the use, asserting that the amount necessary to qualify as a fair use would likely differ based on the use and platform.[228] The proponents of this class nonetheless admit that as a practical matter, file-size limitations for e-books will dictate that only brief excerpts be used.[229] Finally, proponents also cite the Register's previous determination that uses of short clips from motion pictures in multimedia e-books can constitute a noninfringing fair use.[230]

vi. Proposed Class 6: Filmmaking Uses

Joint Filmmakers argue that the proposed uses in both documentary and narrative films are noninfringing fair uses because filmmakers "contribute substantially to society by providing criticism and commentary, educating, and reporting on the news and current events—activities that Congress has explicitly identified as fair uses."[231] But Joint

[224] Authors Alliance Supp. at 7. For example, Jack Lerner, representing Authors Alliance and Buster, asserted that taking even a "huge portion of a film" would very likely be "a slam-dunk fair use" if it were analyzed clip by clip in the context of film studies. Tr. at 31:23-32:07 (May 28, 2015) (Lerner, Authors Alliance/Buster). Commenter FSF also submitted a short comment alleging that the use of clips and still images in multimedia e-books is a fair use. FSF Class 5 Supp. at 1.

[225] Authors Alliance Supp. at 8, 11-13; *id.* at Apps. B-C (describing planned e-books by filmmaker Jilian Spitzmiller, copyright scholar Pamela Samuelson, as well as a volume entitled *Listening to Movies* by sound editor Mark Berger, and a four-part series called *Deconstructing Masters of Cinema* by professor Bobette Buster); *see also* Authors Alliance Reply at 12 (noting that "multimedia e-book authors only seek to make fair use in the form of criticism, commentary, and education").

[226] Authors Alliance Supp. at 11, App. C.

[227] *Id.*at App. B.

[228] Authors Alliance Reply at 11-12 (stating that "what may in practice be considered short in length for a documentary film may not qualify as short for a multimedia e-book").

[229] *See, e.g.*, Tr. at 33:03-07 (May 28, 2015) (Buster).

[230] Authors Alliance Supp. at 7, 9.

[231] Joint Filmmakers Supp. at 5; *see also* NMR Class 6 Supp. at 12 (noting that documentary filmmakers "analyze current events, discuss history, and comment on and criticize popular culture" and use

Filmmakers do not explicitly analyze the proposed uses under the four fair use factors. NMR, however, implicitly suggests that the first and fourth factors favor an exemption when it asserts that the filmmaking uses at issue are transformative because they "add to the original work with a new message."[232] NMR describes numerous examples of actual or prospective uses of motion picture excerpts in documentary films for purposes of film criticism or analysis.[233] Filmmaker Gordon Quinn also briefly mentions that uses of video games in films could qualify as noninfringing fair uses.[234]

Proponents also assert that there is no clear dividing line between documentary and narrative filmmaking for purposes of determining whether the uses are likely to be fair and that the categories should therefore be treated the same with respect to the question of noninfringing use.[235] Joint Filmmakers assert that narrative (*i.e.*, fictional) filmmakers may also "conduct criticism and commentary, using techniques such as parody, reference, and pastiche,"[236] and purport to provide examples of such uses in narrative films.[237] More specifically, Joint Filmmakers submitted a chart entitled "Fair Use in Scripted Films" which lists more than 30 narrative films that they assert successfully relied upon fair use in lieu of obtaining permissions for use of copyrighted works in connection with rights clearance processes or litigation since the 2012 rulemaking.[238] These films were further classified by type, with the overwhelming majority categorized as "Based on a True Story" or "biopics."[239] A few were

---

"copyrighted motion picture material in ways that are excused under fair use"); FSF Class 6 Supp. at 1 (requesting exemption for "filmmaking purposes that do not infringe copyright").

[232] NMR Class 6 Supp. at 14. NMR also contends that "documentary films represent uses that Title 17, Section 107 of the United States Code mandates are protected under fair use." *Id.*

[233] *Id.* (describing *Valentino's Ghost*, which used excerpts of Hollywood films to provide commentary on "Hollywood filmmakers' bigotry and Islamophobia").

[234] Tr. at 109:14-110:13 (May 20, 2015) (Quinn, Kartemquin Educational Films) (describing aborted documentary project that proposed to use high-resolution footage from video games "to talk about their sexism, their violence, other aspects of video games").

[235] *See* NMR Class 6 Supp. at 13 (asserting that "[m]any filmmakers create fictional and nonfictional films that are highly transformative and thus fall under fair use"); NMR Post-Hearing Resp.; Joint Filmmakers Post-Hearing Resp.; *see also* Tr. at 27:15-24 (May 20, 2015) (Perez, Joint Filmmakers); Tr. at 53:21-22 (May 20, 2015) (Neill, NMR).

[236] Joint Filmmakers Supp. at 5; Joint Filmmakers Reply at 3-6 (noting that narrative filmmaking "is a rich and diverse art form that encompasses much more than mere entertainment" and "at its best . . . offers the same thought-provoking insights into and criticisms of the world as the most critically acclaimed literature"); *see also* Tr. at 29:12-20 (May 20, 2015) (Perez, Joint Filmmakers).

[237] *See, e.g.*, Joint Filmmakers Supp. at App. D (Letter from Kenn Rabin), App. F (Letter from Michael Mailer); *id.* at App. G (Letter from Pablo Cruz) (describing the narrative film *Cesar Chavez* and use of footage of actual historical events).

[238] *Id.*at App. C at Chart 2.

[239] While the commenters ultimately disagree about a precise definition of the term "biopic," as discussed further below, Joint Filmmakers initially described biopics as "fact-based narratives [that] present information and commentary meant to educate and analyze real events." *Id.*at 5.

characterized as films "inspired by" real events or what Joint Filmmakers classify as "totally fictional" films.[240]

Joint Filmmakers also rely upon statements by the Register, the Librarian, and NTIA recognizing fair use in filmmaking, at least in certain contexts.[241] Finally, NMR argues that compensation for films is not determinative in evaluating fair use because "[f]ilmmakers who receive compensation for their work still have important messages to communicate to the public and should be able to circumvent TPMs to communicate those messages."[242]

vii. Proposed Class 7: Noncommercial Videos

EFF/OTW assert that the fair use factors generally support a finding that using motion picture clips in remix videos is likely to be noninfringing. Under the first fair use factor, EFF/OTW argue that the purposes and character of noncommercial videos are highly transformative, regardless of whether the videos are also entertaining, and offered scholarly analysis of remix videos characterizing the videos as transformative.[243] In particular, EFF/OTW provide evidence relating to the practices of "vidders," a sub-community of remixers who create fan videos that remix footage from television shows or films into montages set to new soundtracks, at times altering the footage to create various effects.[244] EFF/OTW argue that vidders create works that criticize and recontextualize the underlying narrative works, or make prominent "something latent, hidden or potential in a moving image."[245] While some examples evidenced editing of the visual or audio files themselves, others "mashed up" video images from one source

[240] *Id.*at App. C at Charts 2-4.

[241] *Id.*at 5 (noting that NTIA stated that documentary filmmaking is a "paradigmatic fair use of copyrighted works"); *see also* 2012 Recommendation at 126-30; 2012 Final Rule, 77 Fed. Reg. at 65,268.

[242] NMR Class 6 Supp. at 17; *see also* FSF Class 6 Supp. at 1.

[243] EFF/OTW Reply at 3-5.

[244] EFF/OTW Supp. at 3-4.

[245] *Id.* at 4-5; Tr. at 214:03-08 (May 28, 2015); *see also* EFF/OTW Reply at 3, App. A (explaining that *SupreMacy* "re-tells the James Bond story with M, Bond's female boss and sometime mentor, as the protagonist")

with audio from another,[246] or simply added subtitles over material from a single source.[247]

While focused primarily on the first factor, EFF/OTW argue that the other factors also generally militate in favor of fair use. They claim that the nature of the work weighs "neither for nor against fair use" since both the initial and remix works are likely creative. EFF/OTW contend that the use of short clips is "consistent" with the third factor, and regardless, that case law supports taking "substantial verbatim sections" or even an "entire work" if necessary for the artist's purpose.[248] Fourth, they claim "the transformativeness of remix videos make[s] market harm unlikely."[249] EFF/OTW also point to past rulemakings, which found that a "significant number" of remix uses are likely to be fair because the uses are transformative, noncommercial, and take only short portions of the underlying copyrighted works.[250] EFF/OTW argue that "even fully commercial works are regularly entitled to fair use protection," and that remixers should not be penalized due to receipt of commissions, exhibition payments, or indirect participation in commerce, such as presentation of videos on advertising-supported sites such as YouTube.[251]

[246] EFF/OTW Supp. at App. A at 1 (citing Randy Szuch, *Avatar/Pocahontas Mashup*, VIMEO (Feb. 11, 2010), https://vimeo.com/9389738 ("*Avatar/Pocahontas Mashup*")); *see id.* at App. A at 2 (citing Joe Sabia, *The Rent is Too Damn UP*, POLITICAL REMIX VIDEO (Oct. 19, 2010), http://www.politicalremixvideo.com /2010/10/19/the-rent-is-too-damn-high-up-remix, *available at* https://www.youtube.com/watch?v=ugLKGRmhVTM ("*The Rent is Too Damn UP*")). Proponents also cite a *Ferris Bueller* remix which falls into a similar category. *Id.* at App. A at 1 (citing Rohan Ramakrishnan, *The 10 Best Youtube Trailer Remixes Ever*, SCREENCRAVE (Aug. 4, 2010), http://screencrave.com/2010-08-04/the-10-best-youtube-trailer-remixes-ever ("*Ferris Bueller* Remix")).

[247] *See id.* at App. A at 1, 2-3 (citing The Master, *Top 10 Hitler Downfall Parodies of All Time*, RANKER, http://www.ranker.com/list/top-10-hitler-downfall-parodies-of-all-time/the-master (last visited Oct. 7, 2015) ("The Master") and St01en Collective, *Lord of the Rings: Fellowship of the Ring of Free Trade*, YOUTUBE (Nov. 24, 2006), http://www.youtube.com/watch?v=vkmczhkrKYA, *available at* https://www.youtube.com/watch?v=GNn54ctPwtQ ("St01en Collective's *Lord of the Rings*")).

[248] *Id.* at 6; EFF/OTW Reply at 5 (citing, *e.g.*, *Northland Family Planning Clinic, Inc. v. Ctr. for Bio-Ethical Reform*, 868 F. Supp. 2d 962, 976 (C.D. Cal. 2012); *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 449-50 (1984); *Bill Graham Archives v. Dorling Kindersley Ltd.*, 448 F.3d 605, 609 (2d Cir. 2006)).

[249] EFF/OTW Supp. at 6.

[250] *Id.* at 5-6 (citing 2010 Recommendation at 49-52 and 2012 Recommendation at 127-29).

[251] EFF/OTW Reply at 6-7 (discussing works from the artist collective soda_jerk, the NCAI, the Center for Bio-Ethical Reform, and the Lear Center and citing *Sony*, 464 U.S. at 451; *Princeton Univ. Press v. Mich. Document Servs., Inc.*, 99 F.3d 1381, 1385-86 (6th Cir. 1996); *Campbell*, 510 U.S. at 584; *L.A. News Serv. v. Reuters Television Int'l*, 149 F.3d 987, 994 (9th Cir. 1998)).

c. Asserted Adverse Effects

i. Proposed Class 1: Colleges and Universities

Joint Educators claim that a prohibition on circumvention adversely affects noninfringing educational uses, and that the needs of college and university faculty and students have evolved such that access to higher definition material is necessary. Joint Educators assert that access to Blu-ray clips is now required for cinema studies, providing as an example a lecture on the work of filmmaker Jacques Tati, whose style involves complex compositions contrasting foreground and background action that cannot be appreciated in standard definition ("SD").[252] Proponent Professor Decherney similarly asserts that his current course on the history of Hollywood has a "palpable hole" due to the prohibition on circumvention of Blu-ray discs, explaining, for example, that high-definition quality is necessary to see small details in the *Wizard of Oz* that make the film "really enjoyable and almost stage-like."[253] Proponents refer to other films, such as *Halloween* or *Citizen Kane*, where high definition enables viewers to see additional narrative elements that further the plot, provide commentary, or enhance aesthetics.[254] Beyond Blu-ray, Joint Educators maintain as well that circumvention of DVDs continues to be required, as well as of streaming formats, since certain programming is solely available on streaming platforms.[255]

While most examples in the record concern uses in connection with cinema studies or that would otherwise fall under the prior exemption covering "close analysis of film and media excerpts," Joint Educators nonetheless argue that high-quality images are generally helpful to convey "feelings of presence" for educational uses more generally.[256] Joint Educators also discuss history students viewing the film *Saving Private Ryan*, asserting that it demonstrates the horror of war through use of "a process called bleach bypass, which leaves the silver on the film stock during processing," resulting in "much crisper contrast and color" and through use of "hyper-real details and complex soundscapes" that allegedly would not be adequately captured by a more limited DVD format.[257]

Joint Educators also assert that professors will suffer from time constraints if they are not allowed to circumvent TPMs—because it will take them too long to queue up clips from alternative sources—and that the heightened viewing expectations of students

---

[252] Joint Educators Class 1 Supp. at 7; Joint Educators Class 1 Reply at 12.

[253] Joint Educators Class 1 Supp. at 16; Joint Educators Class 1 Reply at 8-12 (also discussing *Halloween* and *Citizen Kane*).

[254] *Id.*

[255] Joint Educators Class 1 Supp. at 17.

[256] Joint Educators Class 1 Reply at 13.

[257] *See id.* at 15; *see* Tr. at 26:23-27:13 (May 27, 2015) (Band, LCA); Tr. at 29:20-30:05 (May 27, 2015) (Decherney, Joint Educators).

demand high-resolution material to retain attention, convey additional information, and avoid sending the message that lower-quality images reflect less valuable content.[258] Joint Educators contend that these adverse effects, if not catastrophic, are also not *de minimis*.[259] Responding to opposition comments, Joint Educators suggest that the Librarian is authorized to find that grounds of "convenience" or "quality" are sufficient adverse effects under section 1201.[260]

As with prior 1201 rulemakings, Joint Educators dispute the viability of alternatives to circumvention, arguing that screen-capture technology is of poor quality, expensive, and offers limited interoperability.[261] They also object that licensing requirements are unworkable and could inhibit academic freedom due to the inability to get permissions, as well as the cost and length of negotiations.[262] Finally, Joint Educators argue that high-definition digital streaming or films downloaded from licensed sources are not adequate alternatives due to restrictions imposed by user agreements, limited libraries, internet connectivity issues, and logistical difficulties.[263]

Joint Educators also suggest that the exemption should encompass all audiovisual works, instead of being limited to motion pictures, and submit limited evidence suggesting that video games have become the subject of study in university settings.[264] Joint Educators do not, however, provide specific evidence demonstrating that circumvention of TPMs is necessary to use video games as a pedagogical tool. Similarly, while Joint Educators assert that there is no legal requirement that fair uses be limited to "short portions," they do not provide examples where this limitation has prevented noninfringing use of a work.[265]

ii. Proposed Class 2: Primary and Secondary Schools (K-12)

Concerning uses of works in the pre-college setting, proponent Hobbs states that "educational uses that depend upon close analysis of film or media images are adversely impacted if students are unable to apprehend the subtle detail or emotional impact of the images they are analyzing."[266] Hobbs offers the example of a student group creating a hypothetical election campaign for the character Scooby Doo. Unable to legally rip

[258] Joint Educators Class 1 Supp. at 12-16.

[259] Joint Educators Class 1 Reply at 8.

[260] *Id.*

[261] Joint Educators Class 1 Supp. at 18-19; Joint Educators Class 1 Reply at 16-17 (arguing screen-capture technology results in non-standard frames, dropped frames, and a lower quality visual and audio file); *see also* Joint Educators Class 1 Supp. at 20 (re DVD jukeboxes).

[262] Joint Educators Class 1 Supp. at 19.

[263] Joint Educators Class 1 Reply at 18-21.

[264] Joint Educators Class 1 Supp. at 10-11.

[265] Joint Educators Class 1 Reply at 4-5.

[266] Hobbs Class 2 Supp. at 2-3.

DVDs, the students used low-resolution YouTube clips to create an imaginary TV spot. Hobbs argues that the poor image quality created a "diminished sense of pride" for the students.[267] Hobbs further contends that the distinction between high school and college students is arbitrary for purposes of an exemption.[268]

According to Professor Hobbs, "access to high quality images is needed in order for a lesson to accomplish its pedagogical goals," and sometimes, "simply in order for the content to be usable."[269] The proponents of Class 2 also reject alternatives to circumvention as insufficient, arguing that clip libraries are limited, and that screen-capture tools are expensive, unreliable, low quality, and do not provide tools such as closed captioning.[270]

iii. Proposed Class 3: Massive Open Online Courses (MOOCs)

Although MOOCs appear to be expanding in popularity, Joint Educators contend that the prohibition on circumvention of TPMs is inhibiting the introduction of certain types of courses.[271] Specifically, Professor Decherney testified that he has delayed introducing an online version of his *The Hollywood Film Industry* course until an exemption is in place.[272] According to Joint Educators, while tens of thousands of MOOC courses have been offered, only four concern film studies, thus providing circumstantial evidence that the prohibition on circumvention of TPMs on audiovisual works is preventing instructors from making noninfringing uses of clips in online film courses.[273] Joint Educators also urge that because instructors are typically filmed in high definition and students watching an online course are "only a click away" from distraction, high-definition images are especially important for MOOC learning.[274]

Professor Decherney stipulates that only "very short" portions of works will be used, explaining that MOOCs are generally 7 to 10 minutes long and that "[i]t turns out . . . the average time for people to tend to tune out was four minutes and thirty seconds."[275] Joint Educators contend that these time constraints make cueing up multiple clips impossible, and that it is unrealistic to ask students to navigate outside a lesson to view a video on YouTube and then return to the course.[276] Embedding linked content into

[267] *Id.* at 6.

[268] *Id.*; Tr. at 208:16-23 (May 27, 2015) (Hobbs).

[269] Hobbs Class 2 Reply at 6. Hobbs references, but does not provide, a study that allegedly found improved student discussion when analyzing high-quality video compared to screen-captured content.

[270] Hobbs Class 2 Supp. at 7; Hobbs Class 2 Reply at 6-7.

[271] Joint Educators Class 3 Supp. at 17.

[272] *Id.*

[273] Joint Educators Class 3 Reply at 10.

[274] Joint Educators Class 3 Supp. at 11.

[275] Tr. at 115:17-21 (May 27, 2015) (Decherney, Joint Educators); Joint Educators Class 3 Supp. at 9, 15.

[276] Joint Educators Class 3 Supp. at 18.

presentations is also apparently unappealing due to imposition of advertisements by services like YouTube.[277] According to Joint Educators, screen-capture technology degrades the video and audio quality of motion pictures, such that it becomes difficult to optimize MOOCs for the variety of devices necessary for successful delivery.[278] Use of commercial streaming services such as Netflix was also rejected by proponents due to use limitations imposed by providers regardless of fair use rights.[279] Proponents further contend that such streaming services offer limited libraries that are curated for entertainment, not education, and that the rotating catalogs offered by these services are insufficiently reliable for professors who teach consistent classes across semesters.[280]

iv. Proposed Class 4: Educational Programs Operated by Museums, Libraries or Nonprofits

In supporting Proposed Class 4, Professor Hobbs explains that educators and learners in digital learning or media literacy programs are unable to legally circumvent "copy-protected DVDs for informal learning in out-of-school contexts," and lists organizations that are prohibited from accessing such works because "they primarily work in informal learning settings."[281] For example, Hobbs discussed YESPHILLY, a nonprofit GED-conferring organization that could not circumvent TPMs to incorporate DVD clips in a poetry video project; Hobbs notes that, in contrast, film students at nearby universities who hypothetically engage in a similar project could benefit from the existing exemption.[282]

Hobbs argues that screen-captured copies are "inferior" to digitally copied clips, and suggests that screen-capture technology does not always work with streaming services.[283] She also states that streaming media platforms such as Discovery Education, with annual fees up to $10,000, are cost prohibitive for many nonprofit educators and are of limited use without reliable high-speed internet access.[284]

---

[277] Joint Educators Class 3 Reply at 19.

[278] *Id.* at 14-16.

[279] *Id.* at 14-17.

[280] *Id.* at 18.

[281] Hobbs Class 4 Supp. at 2, 4.

[282] Hobbs Class 4 Reply at 5; *see also* Tr. at 259:08-25 (May 27, 2015) (Hobbs) (discussing a nonprofit organization that was barred engaging in a project to excerpt and comment on clips depicting misogynistic representations in contemporary culture).

[283] Hobbs Class 4 Reply at 5, 7-8 (asserting that "screencasting does not always work when using encrypted DVDs, Blu-Ray discs, Netflix, Amazon Prime, Roku, Hulu Plus, or other streaming services"); Tr. at 171:04-06 (May 27, 2015) (Hobbs) (stating that "Screencast-O-Matic and Camtasia" screen capture programs were unable to capture "Wolf Hall" on PBS streaming).

[284] Hobbs Class 4 Reply at 7.

v. Proposed Class 5: Multimedia E-Books

In seeking an exemption for multimedia e-books, Authors Alliance argues that prohibiting circumvention of CSS encryption on DVDs would "severely hinder[] authors' ability to criticize and comment on important protected material from DVDs," which sometimes are the only source of material.[285] Similarly, they contend that "a significant and increasing amount of motion picture material is available only through digitally transmitted video sources," such as streaming or broadcast television.[286]

Concerning Blu-ray, Authors Alliance argues that there is a "substantial and increasing amount of motion picture material . . . available exclusively on AACS-protected Blu-Ray."[287] Proponents claim that standard-definition files are not always suitable because they "cannot convey the [desired] detail, clarity, and content," have unacceptable sound quality, are distracting to viewers, and can "degrade over time."[288] Authors Alliance cites as an example law professor Pamela Samuelson's study of the copyrightability of the James Bond character, asserting that high-quality source material is necessary to allow "students to take a fine-grained look at the development of James Bond's character," including his watch, his age, and his dress.[289] In addition, Authors Alliance argues that high definition "has become the prevailing standard for rendering video on modern e-reader devices," and is "now the baseline of acceptable quality for multimedia e-books."[290] As evidence of that claim, proponents assert that Apple's "quality control is very strict and . . . there's a serious and reasonable fear that without HD content, Apple will reject quite a number of books" for its iBooks platform.[291]

---

[285] Authors Alliance Supp. at 11 (noting that "DVDs are still among the most common sources of motion picture material, and at times, the only source"). FSF also asserts that "[t]he application of the right to fair use. . . is impeded by access control restrictions which prevent the creators of Multimedia E-Books from taking clips and still images from other audiovisual works." FSF Class 5 Supp. at 1.

[286] Authors Alliance Supp. at 14-15 (citing example of material unavailable on DVD).

[287] *Id.* at 12; *see also id.* at App. E.

[288] Authors Alliance Reply at 6; Authors Alliance Supp. at 13, App. C; *see also* Authors Alliance Supp. at App. B at 1 (providing the example of Professor Bobette Buster, who stated that the "consumer expects, even demands the highest affordable quality of viewing and listening experience" and that, with lower quality DVDs, she is forced to "describe fully what the class should be experiencing from the filmmaker's original vision"); Tr. at 37:07-12 (May 28, 2015) (Buster) (asserting that "films have been mixed with either 5.1, 7.1, or, at most, surround sound. HD promises the right levels of mixture of that, and what I see with SD is that it's sort of generically mixed and some levels are too high, some are too low"); Tr. at 17:09-12, 25:17-19 (May 28, 2015) (Buster); Tr. at 76:04-77:01 (May 28, 2015) (Benmark, Authors Alliance/Buster).

[289] Authors Alliance Supp. at 12; *see also id.* at App. C (noting that "[a] major problem with lower-fidelity formats is that they utilize increasing degrees of compression," which "sacrifices the video and audio quality").

[290] Authors Alliance Reply at 6.

[291] Tr. at 106:17-20 (May 28, 2015) (Lerner, Authors Alliance/Buster); *see also id.* at 10:21-11:11 (Buster). iBooks Author is an app that allows people to create and publish e-books for Apple products. *iBooks Author*, APPLE, https://www.apple.com/ibooks-author (last visited Oct. 7, 2015).

Proponents object to alternatives to circumvention as costly, impracticable, inferior, and unduly burdensome.[292] Screen-capture software is described as "impossibly difficult for authors to operate"[293] and of unacceptably low quality.[294] Finally, it contends that "many authors" use Apple computers, which "will just flat block any screen-capture program from working with a TPM-protected or encrypted disk."[295]

Finally, Authors Alliance contends that licensing is "an unrealistic option" because nearly all major studio licenses charge "exorbitant fee[s]" and "bar[] licensees from casting the studio or the film in a negative light."[296] In other cases, self-publishing authors "are often unable to find the rightsholder, receive permission, or create a legally binding agreement."[297]

vi. Proposed Class 6: Filmmaking Uses

Joint Filmmakers contend that the proposed exemption for filmmaking is necessary lest filmmakers be "forced to self-censor their work because they often cannot obtain a usable copy [free of TPMs] of a copyrighted work for fair use."[298] They state that "much of the material filmmakers need is still only available on DVD."[299] Joint Filmmakers also contend that filmmakers require access to digitally transmitted video, including material on cable television, Netflix, Hulu, YouTube, iTunes and other online distribution sources, because some of this material "can only be obtained online" or is not yet available on discs.[300]

While asserting the need for an exemption to cover DVD and online video sources, Joint Filmmakers at the same time seek to access Blu-ray source material, claiming that "Blu-Ray is quickly supplanting DVD as the predominant source of motion

---

[292] Authors Alliance Supp. at 15 (cost of visual stabilizers, digital time base correctors and film editing software); Authors Alliance Reply at 6, 9.

[293] Authors Alliance Supp. at 16; *see also* Tr. at 73:20-74:06 (May 28, 2015) (Benmark, Authors Alliance/Buster).

[294] *See* Authors Alliance Reply at 10-11; Tr. at 73:06-18 (May 28, 2015) (Benmark, Authors Alliance/Buster). Authors Alliance questioned whether screen-capture software, such as WM Capture or Greenshot, could adequately work with many types of TPMs.

[295] Tr. at 73:02-05 (May 28, 2015) (Benmark, Authors Alliance/Buster); *see also id.* at 75:14-21 (Benmark, Authors Alliance/Buster).

[296] Authors Alliance Supp. at 17; *see also* Authors Alliance Reply at 9. Authors Alliance also asserts that "[a]bsent the ability to make fair use, many authors would be prohibited from using copyrighted material merely because the rightsholder disapproves of the authors' message." Authors Alliance Supp. at 17-18.

[297] Authors Alliance Reply at 9.

[298] Joint Filmmakers Supp. at 7-8, App. C at 2; *see also* NMR Class 6 Supp. at 12.

[299] Joint Filmmakers Supp. at 8; *see also id.* at App. I.

[300] *Id.* at 11, App. B at 4, App. K. Joint Filmmakers also cited filmmaker Danny Yourd as an example where using a DVR to collect news clips is needed to easily obtain high-definition clips and clear them for "E+O and distribution." *Id.* at 12.

picture material, especially high quality HD material and bonus footage."[301] Without such access, NMR suggests that documentarians would "have to forego using that content," interfering with filmmakers' ability to communicate their intended message.[302] Proponents contend that high-definition content is necessary to more effectively engage in comment and criticism. For example, Gravitas Films allegedly required Blu-ray sources for a documentary about the film industry that "compare[d] the fine grained details of existing motion pictures, . . . [that] cannot be found on standard definition DVDs."[303]

Separate and apart from the artistic needs of filmmakers, Joint Filmmakers claim that industry distribution standards establish that "[h]igh definition footage is mandatory in the modern filmmaking and broadcasting world."[304] They explain that broadcasters and film distributors require high-definition or better-quality footage, and will "reject projects that do not meet these stringent standards, even in the conceptual stage."[305] According to Jim Morrissette of Kartemquin Educational Films, broadcasters like CNN, PBS, BBC and NBC Universal perform technical quality control on programs that "analyzes every frame for video defects that do not meet their stringent technical requirements."[306] Joint Filmmakers also contend that films will be rejected by theatrical exhibitors, film festivals, and other venues unless they use high-quality footage.[307] Even

[301] *Id.* at 10, App. B at 4-5, App. K.

[302] NMR Class 6 Supp. at 16.

[303] Joint Filmmakers Supp. at 10; *see also* NMR Class 6 Supp. at 16 (noting that low quality excerpts "provide less detail and less information"); Joint Filmmakers Supp. at App. D at 5; Tr. at 25:03-23 (May 20, 2015) (Quinn, Kartemquin Educational Films).

[304] Joint Filmmakers Reply at 7; *see also* Joint Filmmakers Supp. at App. B at 1; Tr. at 51:06-18 (May 20, 2015) (Neill, NMR).

[305] Joint Filmmakers Reply at 7-8. Morrissette asserts that multiple standard-definition archival clips in a documentary film submitted to CNN were rejected because they contained "thick black lines around the image, dropped frames, interlace artifacts" and other problems, all of which "proved to be unfixable, even after extensive and costly processing, and had to be removed from the movie simply because they failed quality control." *Id.* at App. B at 1; *see also id.* at App. C, App. E (stating that the PBS show, *Independent Lens*, which showcases independent documentaries, requires delivery of high-definition films on "HDCAM 1080i, 59.94 drop frame"); Joint Filmmakers Supp. at App. I at 1 (statement of Joel Schroeder) (noting that in order to deliver a film to Discovery or CBS, "the standard has to be at least a master of 1080p or 29.9 FPS"). According to Joint Filmakers, not only does PBS accept only HD programs, but NBC and CNN also have "equally high standards for footage" and reject standard-definition clips or clips suffering from image framing errors that proponents assert are common to screen-capture software. Joint Filmmakers Reply at 8-9, App. D; Tr. at 9:21-23 (May 20, 2015) (Morrissette, Kartemquin Educational Films).

[306] Joint Filmmakers Reply at App. B at 1.

[307] Joint Filmmakers Supp. at App. B at 1 (noting that over "90% of all movie theaters in the US now have digital projection, in either 2K resolution (1920x1080 pixels) or 4K resolution (3840x2160 pixels)," requiring files "over anything a standard definition DVD (720x480 pixels) can adequately deliver."); *id.* at 10 (noting Finite Films was required to use 1080p (*i.e.*, Blu-ray level) resolution by film festivals, also referencing marketplace events, screenings, and seminars); *id.* at App. H; *see also* NMR Class 6 Supp. at 16 (quoting documentarian Rick Bowman claiming "at this past year's American Film Market event in Los Angeles, distributors didn't want to look at any films unless they had been filmed in 4K").

when not strictly required for distribution, NMR argues that documentary filmmakers must access high-definition video content because high definition is generally expected by audiences, whereas low-quality content "deters audiences from viewing documentaries."[308] Moreover, Joint Filmmakers explain that "everyone is now producing in 4K"—referring to 4K resolution, which offers four times the resolution of Blu-ray—and that DVD quality will not "stand up" as use of 4K resolution becomes widespread.[309]

Joint Filmmakers explain that "upconverting" DVD standard-definition clips to meet the pixel ratio of an otherwise HD-quality film "severely degrades the footage's quality," and creates "fake" frames that "behave differently than the actual frames from the DVD" or high-definition images.[310] By way of analogy, they evoke the image of a drivers' license picture stretched across the length of a movie poster (in the case of HD) or a billboard (in the case of 4K resolution).[311] In any event, proponents assert that upconversion tools are often "entirely unavailable, too cost prohibitive, or too difficult to operate."[312]

Joint Filmmakers claim alternatives to circumvention are not reasonably available.[313] According to Joint Filmmakers, solutions like using a smartphone camera to record images displayed on a screen result in video quality "degraded so significantly as to be unusable," and that such images cannot convey the filmmaker's vision or meet the technical standards of distributors.[314] Joint Filmmakers assert that opponent DVD CCA's exhibits of screen-captured clips "would be rejected by modern distributors and broadcasters" and would "not allow the type of detailed criticism and commentary that many filmmakers need to undertake."[315] In addition, they claim that screen-capture

[308] NMR Class 6 Supp. at 15. NMR also argued that a "documentary filmmaker's ability to communicate their message effectively depends on the quality of the video content that the filmmaker uses." *Id.*

[309] Tr. at 11:01-23 (May 20, 2015) (Morrissette, Kartemquin Educational Films).

[310] Joint Filmmakers Supp. at App. B at 1-2; *see also id.* at 12; Tr. at 98:23-99:06 (May 20, 2015) (Morrissette, Kartemquin Educational Films). The process of upconverting a standard-definition DVD (720 x 480 pixels) to high definition (1920x1080 pixels) involves adding additional "fake" pixels between the real pixels using a video hardware box. Additional processing would be required to convert that file into a format that would play on digital theater projectors or an ultra-high-definition ("UHD") TV. *See* Joint Filmmakers Supp. at App. B at 1-2.

[311] Joint Filmmakers Supp. at 10-11.

[312] *Id.* at 12, App. B at 1-2; *see also* Tr. at 98:23-99:06 (May 20, 2015) (Morrissette, Kartemquin Educational Films); Tr. at 101:14-102:02 (May 20, 2015) (Lerner, Joint Filmmakers).

[313] Joint Filmmakers Supp. at 12.

[314] *See id.* at 12-13, App. B at 3; Joint Filmmakers Reply at 10-11; *see also* Joint Filmmakers Reply at App. B at 1-2 (stating that filming a television with a camera or cellphone "creates Moire interference, a visual distortion effect created by the interaction of the camera image sensor and the pixels of the TV screen" that "renders the resulting image fuzzy and completely unsuitable for broadcast").

[315] Joint Filmmakers Reply at 11-12, App. F (explaining that the *Matrix Reloaded* clip captured from a DVD is unacceptable because the WMCapture software is unlikely to be able to "handle playing and recording simultaneously 29.97 frames per second of 1080p footage"); *see also* Joint Filmmakers Supp. at

software "presents a real question of legality to filmmakers . . . because it is not clear whether the copyrighted material is captured before or after decryption."[316] They also claim that screen-capture software is not "available for Blu-ray on the Mac platform used by a majority of filmmakers."[317]

According to Joint Filmmakers, licensing is not a viable option because rightsholders often fail to respond or "deny permission based on the content of the intended use."[318] In addition, they claim that licensing can be cost prohibitive.[319]

vii. Proposed Class 7: Noncommercial Videos

According to NMR, previous legal battles demonstrate that many remix videos "would not even exist" without the existing exemption, proving adverse impact.[320] EFF/OTW similarly claim that, but for an exemption, creators who could otherwise contest improper DMCA takedown notices will be prevented from doing so because of the prohibition on circumvention.[321] In contrast, remixers who counter-notify under the DMCA or contest a YouTube Content ID match are typically successful, suggesting that section 1201 stifles the dissemination of noninfringing uses.[322] EFF/OTW further contend that section 1201 is unfamiliar to remixers, so the provision creates "a set of perverse incentives and traps for the unwary."[323]

Proponents argue that all potential alternatives to circumvention are inadequate, focusing in particular on their claim that any exemption should include circumvention of Blu-ray discs protected by AACS. According to proponents, much material is available only from a single source, such as Blu-ray or online.[324] Further, Blu-ray "bonus"

---

13 (noting that screen capture software "still has unacceptable stuttering, dropped frames, and image size issues"); Tr. at 12:02-24 (May 20, 2015) (Morrissette, Kartemquin Educational Films).

316 Joint Filmmakers Supp. at 13; *see also* Joint Filmmakers Reply at 12 (stating that none of the screen capture programs listed by opponents represent that they enable "the reproduction of motion picture content after such content has been lawfully decrypted").

317 Joint Filmmakers Supp. at 13; *see also id.* at App. B at 3.

318 *Id.* at 13-14; *see also* NMR Class 6 Supp. at 15 (referencing use of clips in film criticizing Hollywood); Joint Filmmakers Reply at 10. Joint Filmmakers point to examples where filmmakers attempted to license clips but were turned down, either with no explanation or because the rightsholder did not agree with the way the clips were used, sometimes for political or financial reasons. *See, e.g.*, Joint Filmmakers Supp. at 13; Joint Filmmakers Reply at 10.

319 Joint Filmmakers Reply at 10.

320 NMR Supp. at 5-6 (discussing *Buffy v. Edward* clip and legal dispute between remix creator and Lionsgate Entertainment, which controlled footage to the television show *Buffy the Vampire Slayer*).

321 EFF/OTW Supp. at 7, 10; Tr. at 245:13-21 (May 28, 2015) (Tushnet, OTW) (asserting that section 1201 creates a chilling effect that prevents remixers from submitting DMCA counter-notifications or litigating).

322 EFF/OTW Supp. at 10-11; *see also* NMR Supp. at 3 (same).

323 EFF/OTW Supp. at 7, 10.

324 *Id.* at 11-12; EFF/OTW Reply at 8-10; NMR Supp. at 10; Tr. at 196:13-197:18 (May 28, 2015) (Charlesworth, USCO; McSherry, EFF).

material, while ancillary to the original copyrighted work, is allegedly often uniquely valuable to a vidder's project of examining and critiquing assumptions in the original work.[325] EFF/OTW also contend that remix artists should be allowed access to the highest quality of source material desired, arguing that the ability to make such aesthetic choices goes to the "heart of copyright."[326] EFF/OTW point to a variety of remix videos made using Blu-ray source material, claiming the material was necessary and offered advantages over other formats due to the ability to portray finer-grained details; accept application of editing effects, including cropping, zooming, or superimposition; and format films with the desired aspect ratio for editing purposes.[327] Conversely, EFF/OTW contend that DVD source material results in lost frames, grainy colors, pixellation and other artifacts that hinder or even preclude desired editing.[328]

EFF/OTW also contest the ability of screen-capture software to capture source material with adequate clarity, audio, and formatting.[329] As an example, EFF/OTW analyze a high-definition video commissioned by NCAI entitled *Take It Away*, which features clips of the Washington Redskins football team, but with the team name and logo removed, to demonstrate that the football viewing experience would remain constant even with the removal of the allegedly disparaging trademark.[330] They note that opponents' attempt to recreate that video using screen-captured footage actually proves this point, asserting that opponents' version is so blurry that "NCAI's point that the logo is unnecessary to a high-quality experience is completely lost."[331] Finally, EFF/OTW contend that even screen-capture technology may implicate circumvention of TPMs.[332]

---

[325] EFF/OTW Reply at 10; Tr. at 210:05-211:04 (May 28, 2015) (Coppa, OTW).

[326] EFF/OTW Supp. at 13-17 (citing *Campbell*, 510 U.S. at 582-83 (quoting *Bleistein v. Donaldson Lithographing Co.*, 188 U.S. 239, 251 (1903)) ("It would be a dangerous undertaking for persons trained only to the law to constitute themselves final judges of the worth of [a work], outside of the narrowest and most obvious limits. At the one extreme, some works of genius would be sure to miss appreciation. Their very novelty would make them repulsive until the public had learned the new language in which their author spoke.")); *see* NMR Supp. at 7-9; EFF/OTW Reply at 11 (citing *Campbell*, 510 U.S. at 588; *Bill Graham*, 448 F.3d at 613; *Warren Pub. Co. v. Spurlock*, 645 F. Supp. 2d 402, 420, 425 (E.D. Pa. 2009)).

[327] EFF/OTW Reply at 10, App. A at 4-6, 11-15 (citing, among others, Jetpack Monkey, *White Telephone*; Rhoboat, *Supremacy*; astrolat and Speranza, *Anything for Love*); EFF/OTW Supp. at 17; Tr. at 206:14-207:02 (May 28, 2015) (Coppa, OTW).

[328] EFF/OTW Reply at 8-10, Apps. A-B. EFF/OTW also submitted a list of materials available only through Blu-ray, compared to DVD.

[329] *Id.* at 8-9; *see also* EFF/OTW Post-Hearing Resp. at 2-7 (disputing that opponents' exhibits represented adequate alternatives).

[330] *See* NCAI Supp. at 1; EFF/OTW Supp. at 9.

[331] EFF/OTW Reply at 11-16; *see also* NMR Supp. at 7-9 (same re *Buffy v. Edward*).

[332] EFF/OTW Supp. at 18-19; Tr. at 243:11-17 (May 28, 2015) (Tushnet, OTW) (stating WM Capture is "the only software that claims not to be circumvention").

d. Argument Under Statutory Factors

i. Proposed Class 1: Colleges and Universities

Joint Educators argue that the statutory factors set forth in section 1201(a)(1) favor the granting of an exemption for college and university uses. With respect to first two factors—the availability for use of copyrighted works and the availability for use of works for nonprofit archival, preservation, and educational purposes—Joint Educators note that many college and university libraries and programs have lawfully acquired extensive motion picture collections. The prohibition on exemption, however, could prevent faculty and students from using these works for educational purposes in a meaningful way.[333] Under the third factor, the impact on criticism, comment, news reporting, teaching, scholarship, or research, Joint Educators assert that the prohibition on circumvention inhibits students and professors from engaging in certain types of instruction, analysis, commentary and criticism.[334] In particular, they observe that low-quality images discourage professors and students from incorporating works obtained from alternative sources into their teaching and scholarship.[335] Finally, under the fourth factor, Joint Educators argue that uses of short clips are unlikely to affect the value of the copyrighted work since the clips are "limited in duration and not likely to serve as a substitute for the entire work."[336] They also state that because previously granted exemptions did not affect the market for copyrighted works, an expanded exemption encompassing Blu-ray discs is also unlikely to have a negative impact.[337]

ii. Proposed Class 2: Primary and Secondary Schools (K-12)

While not explicitly addressing the statutory factors, Hobbs' various submissions strongly stress the educational purpose of this exemption and its relationship to criticism, comment, and scholarship. Hobbs also contends that there would be no effect on the market for the copyrighted works.[338] In addition, perhaps falling into the category of "other factors" that the Librarian may consider, Hobbs cites a study purportedly concluding that use of digital media studies reduces disciplinary problems and minimizes technology skill gaps between lower-income and wealthier students.[339]

---

[333] Joint Educators Class 1 Supp. at 21.

[334] *Id.*

[335] *Id.* at 22.

[336] *Id.*

[337] Joint Educators Class 1 Reply at 22-23.

[338] Hobbs Class 2 Supp. at 3, 9.

[339] Hobbs Class 2 Reply at 4.

iii. Proposed Class 3: Massive Open Online Courses (MOOCs)

Joint Educators maintain that the statutory factors support granting an exemption because (1) works stored on TPM-encumbered formats are unavailable for educational uses; (2) the works are generally lawfully obtained by colleges or universities, and Congress has favored educational uses of audiovisual material, as evidenced by sections 107 and 110 of the Copyright Act; (3) the prohibition on circumvention inhibits the production of and participation in MOOCs and could slow its growth as an educational medium; and (4) as the content would be limited to short clips for educational purposes, using in large part resources previously acquired by a "home institution" university, the market for the underlying copyrighted works is unlikely to be affected.[340]

iv. Proposed Class 4: Educational Programs Operated by Museums, Libraries or Nonprofits

Hobbs did not directly address section 1201(a)(1)'s statutory factors in her comments in support of this proposed exemption.[341]

v. Proposed Class 5: Multimedia E-Books

Authors Alliance argues that the statutory factors support granting an exemption. First, they claim an exemption would allow e-book authors "to use material that they should be able to access under fair use."[342] Second, they note that the Register previously found that "[m]ultimedia e-books have a similar education value [to documentary films] and are intrinsically archival."[343] Third, according to proponents, multimedia e-books make "use of innovative technologies to provide scholarly research and arguments" and "serve as compelling examples of . . . critical scholarship."[344] Finally, proponents claim there will be no adverse effect on the market for copyrighted works, given that there are no "allegations that previous exemptions pertaining to DVDs have resulted in infringing uses."[345] As for other factors that the Register and Librarian could consider appropriate, they contend that the exemption should be granted because, as previously found relevant by the Register, "the TPMs at issue are not used to prevent unauthorized access or to conceal copyrighted material" but instead are being used to

[340] Joint Educators Class 3 Supp. at 21-22; Joint Educators Class 3 Reply at 19-21.

[341] *See* Hobbs Class 4 Supp. at 4-5 (instead addressing section 107's statutory factors to determine fair use).

[342] Authors Alliance Supp. at 18-21; Authors Alliance Reply at 11.

[343] Authors Alliance Supp. at 21; *see also* 2012 Recommendation at 136 (noting for "the availability for use for nonprofit archival, preservation, and educational uses, the focus on education is, of course, relevant to the proposals relating to educational uses, as well as to a lesser degree those relating to documentary films, documentary videos, and multimedia e-books offering film criticism"); Authors Alliance Reply at 11.

[344] Authors Alliance Supp. at 22; Authors Alliance Reply at 11.

[345] Authors Alliance Supp. at 22-23; *see also* Authors Alliance Reply at 8.

"manage rights and to prevent the public from engaging in lawful, noninfringing, and fair uses."[346]

vi. Proposed Class 6: Filmmaking Uses

Joint Filmmakers argue that the statutory factors support granting an exemption for the proposed filmmaking uses. First, they contend that denying an exemption will "severely reduce the availability for use of copyrighted works," by limiting legitimate filmmaking uses.[347] Second, Joint Filmmakers assert that both documentary films and narrative films make uses that "fulfill educational and archival purposes" and are "critical to educational efforts."[348] Third, they state that documentary films are "important sources of criticism, commentary, and in-depth reporting on issues that may otherwise not be widely known," while narrative films "provide important social commentary and help to educate American moviegoers as to important events," all of which would be adversely affected and hindered by prohibiting circumvention.[349] Joint Filmmakers also argue that there is no evidence of any likely harm to the market for DVDs, or, by analogy, Blu-ray discs, because in the last eight years in which DVDs have been covered by an exemption, opponents have "provided neither allegation nor evidence of infringement or harm," and, furthermore, no longer oppose the exemption as it applies to DVDs.[350]

vii. Proposed Class 7: Noncommercial Videos

EFF/OTW argue that each of the statutory factors favors an exemption for noncommercial videos. First, EFF/OTW note that DVDs continue to be well established in the marketplace despite the wide availability of circumvention technology, and from this fact extrapolate that the ability to circumvent does not affect the availability of the underlying copyrighted works.[351] Second, EFF/OTW argue that an exemption would facilitate the preservation and use of remix videos in museums, other cultural institutions, and educational settings.[352] Third, EFF/OTW claim that because remix video creators use their works to engage in criticism and commentary, denying an exemption would inhibit criticism and comment.[353] Fourth, EFF/OTW argue that an exemption would not impact the market or the value of the underlying copyrighted works, noting both the lack

[346] Authors Alliance Supp. at 23; Authors Alliance Reply at 11.

[347] Joint Filmmakers Supp. at 14-17. In support of this point, Joint Filmmakers also assert that an exemption would not decrease the consumption of the underlying works, and point out that in some cases, such as documentaries about feature films, the new work can increase audience appetite for the underlying works. *Id.*

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

[349] *Id.* at 18.

[350] Joint Filmmakers Reply at 9; Joint Filmmakers Supp. at 18.

[351] EFF/OTW Supp. at 19-20.

[352] *Id.* at 20.

[353] *Id.* at 20-21.

of effect seen from prior exemptions as well as the acknowledged acceptance of fan-made works by organizations such as the MPAA.[354]

EFF/OTW also suggest that the Register should avoid "discrimination based on perceived artistic needs" and should not limit an exemption to noncommercial uses.[355] As support, they provide examples of videos distributed in a museum or commissioned for pay.[356] At the hearing, however, Professor Tushnet of the OTW acknowledged that a workable exemption could be limited to "primarily noncommercial" uses if the rule included accompanying guidance explaining what types of activity might be permitted.[357]

2. Opposition

For all of these audiovisual classes, the Office received no opposition to the "renewal" of the current exemptions; instead, opponents focused their comments on containing the existing exemptions without expansion. The same parties oppose all seven classes—Joint Creators,[358] DVD Copy Control Association ("DVD CCA"), and the Advanced Access Content System Licensing Administrator ("AACS LA"). In certain classes, DVD CCA and AACS LA filed joint comments. Opponents voice parallel concerns across most of these audiovisual classes.

Opponents generally contend that there are viable alternatives to circumvention that are adequate for any proposed uses that are not permitted under an existing exemption. Joint Creators and DVD CCA claim that the past three years witnessed significantly improved alternatives to circumvention, including clip licensing, screen-capture technology, streaming platforms such as TV Everywhere, disc-to-digital services, and digital rights libraries like UltraViolet, that enable proponents to easily and affordably copy short portions of motion pictures without circumvention of any access controls.[359] Opponents suggest screen-capture software in particular has "developed significantly over the past three years into an effective tool that allows users to appropriate high quality, broadly compatible images and video."[360] As evidence,

---

[354] *Id.* at 21.

[355] *Id.* at 22 ("Today's bad vid may lead to tomorrow's work of searing cultural criticism.").

[356] *Id.* at 22-23.

[357] Tr. at 310:09-311:12 (May 28, 2015) (Charlesworth, USCO; Tushnet, OTW).

[358] The trade groups represented by Joint Creators are the Motion Picture Association of America, the Entertainment Software Association, and the Recording Industry Association of America.

[359] *See, e.g.*, Joint Creators Class 1 Opp'n at 4-6, 9-11; DVD CCA Class 1 Opp'n at 7-12; Tr. at 198:11-16 (May 27, 2015) (Williams, Joint Creators); Joint Creators Class 2 Opp'n at 6-7 & n.16, 8-11 (listing alternatives, including PBS LearningMedia, YouTube, Anyclip.com, Vudu, UltraViolet, Disney Movies Anywhere, "TV Everywhere" initiatives like online and mobile app offerings from Comcast's XFINITY, Dish Network's DISH Online, and Verizon's FiOS TV Online, and download and streaming platforms such as Apple's iTunes, Amazon Prime, Netflix, Hulu Plus, and AT&T U-verse Live TV); Joint Creators Class 5 Opp'n at 4-6, Exhibits 1-12.

[360] AACS LA Class 2 Opp'n at 9; DVD CCA Class 2 Opp'n at 8-9.

opponents provided screen-captured clips from the films *The Matrix Reloaded* and *Chicago*, and compilations of clips from other motion pictures depicting medieval life and the works of Shakespeare.[361] In response to claims that such alternatives do not provide sufficiently high-quality excerpts, Joint Creators, DVD CCA and AACS each cite *Universal City Studios v. Corley* for the proposition that fair use does not entitle a user of the copyrighted work to "copying by the optimum method or in the identical format of the original."[362]

In response to proponents' claims that the exemptions should, for the first time, be expanded to encompass Blu-ray, AACS LA and Joint Creators contend that the authorized circumvention of DVDs or online material provide a ready alternative to circumvention of Blu-ray discs, particularly because "most of the examples provided in the proponents' comments relate to DVD quality."[363] AACS LA also points out that the DVD market continues to outstrip the Blu-ray market and states that any harm resulting from inferior quality images is speculative.[364] In addition, AACS LA and Joint Creators contend that the amount of material available on Blu-ray alone is *de minimis.*[365]

Both AACS LA and DVD CCS also argue that expanding the exemptions any further will harm the DVD and Blu-ray disc markets.[366] AACS LA warns that circumvention of Blu-ray discs results in a perfect copy of the entire work "in the clear"—that is, free from any restrictions on further copying or redistribution—which it contends could undermine the Blu-ray business model at a time when it still competes with DVD and other distribution models.[367] DVD CCA also voices the concern that

---

[361] *See, e.g.*, AACS LA Class 2 Opp'n at 9-11; DVD CCA Class 2 Opp'n at 9-11; DVD CCA Class 5 Opp'n at 8-11; DVD CCA Class 6 Opp'n at 15-18.

[362] *See, e.g.*, AACS LA Class 1 Opp'n at 6-7 (citing *Corley*, 273 F.3d 429, 459 (2d Cir. 2001)); DVD CCA Class 1 Opp'n at 6-7 (same); Joint Creators Class 1 Opp'n at 8 (same). Opponents also rely upon *U.S. v. Elcom Ltd.*, 203 F. Supp. 2d 1111 (N.D. Ca. 2002) and *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085 (N.D. Ca. 2004) for this point in their submissions.

[363] *See, e.g.*, AACS LA Class 1 Opp'n at 9-13; *see also* Tr. at 225:20-226:02 (May 27, 2015) (Williams, Joint Creators); Joint Creators Class 2 Opp'n at 5. Joint Creators also question whether the phrase "online distribution services" includes online streaming services, such as Netflix, or whether the exemptions were meant to be limited to digital download services such as Apple's iTunes Store, and suggest "digitally transmitted material" may more accurately capture both services. Tr. at 306:17- 308:01 (May 28, 2015) (Williams, Joint Creators; Smith, USCO). *See* 37 C.F.R. § 201.40(b)(4)-(7).

[364] AACS Class 1 Opp'n at 8; AACS LA Class 5 Opp'n at 7, 9; AACS LA Class 6 Opp'n at 10.

[365] *See, e.g.*, AACS Class 7 Opp'n at 2; Joint Creators Class 7 Opp'n at 5.

[366] *See, e.g.*, DVD CCA/AACS LA Class 3 Opp'n at 14; Tr. at 128:02-16 (May 27, 2015) (Turnbull, DVD CCA/AACS LA) (stating that "the concern that we have with the kinds of unbounded exemptions, like the MOOC one that's here, is in fact that it would undermine the licensing system and would thereby undermine the copyright owners' trust in the licensing system and the system of licensed products that are deployed"); *see also* Joint Creators Class 6 Opp'n at 6.

[367] *See, e.g.*, DVD CCA/AACS LA Class 3 Opp'n at 14-16 (asserting that circumvention could undermine "the continued growth of the market for Blu-Ray discs"); AACS LA Class 6 Opp'n at 22; AACS LA Class 7 Opp'n at 16-19.

increased circumvention of DVDs could result in the erosion of a still "widely popular" DVD market.[368]

Opponents contest other attempts to broaden the language of the existing exemptions. Joint Creators object that no proponents have demonstrated a need to expand the exemption to audiovisual works beyond "motion pictures" (such as to video games), or to engage in circumvention for purposes other than for close analysis of film and media excerpts.[369] They also request that the current limitation for uses of "short portions" be retained. Joint Creators, AACS LA and DVD CCA also all object to extending exemptions to "fair uses" or "educational uses" in general, asserting that not all educational uses qualify as fair uses and that a use's simply being educational does not obviate the need for a full analysis of the four fair use factors.[370] The opponents contend that there is a lack of "sufficient description to determine whether any possible activity, which could claim educational purpose, is indeed noninfringing,"[371] arguing that proponents have failed to prove that the full range of desired activities is noninfringing.[372]

Finally, Joint Creators state that TPMs, including AACS and CSS, have proven value and have "increased the availability of works and have allowed for a vast proliferation of platforms" for content distribution.[373] Explaining that "more works than ever are more readily available than ever, in particular through streaming and downloadable online content," Joint Creators attribute such availability to "the legislative promise of secure and robust protection for such content."[374]

---

[368] *See, e.g.*, DVD CCA Class 1 Opp'n at 12-13 (expressing concern for CSS-protected discs); *see also* Tr. at 127:20-128:01 (May 27, 2015) (Turnbull, DVD CCA/AACS LA) (noting that "a judge in California found that an effort to make a movie library was indeed irreparable harm to the DVD CCA licensing system").

[369] Joint Creators Class 1 Opp'n at 5; Joint Creators Class 3 Opp'n at 8; Joint Creators Class 5 Opp'n at 6; Joint Creators Class 6 Opp'n at 6; Tr. at 93:07-16 (May 28, 2015) (Williams, Joint Creators).

[370] *See, e.g.*, Joint Creators Class 1 Opp'n at 4 (also arguing in favor of preserving "short portions" limitation); AACS LA Class 1 Opp'n at 5 (citing 2012 Recommendation at 140); DVD CCA Class 1 Opp'n at 3-5; Joint Creators Class 2 Opp'n at 3-4 (noting that "the four statutory factors must be fully evaluated in view of the facts of any particular use").

[371] AACS LA Class 2 Opp'n at 5; *see also* DVD CCA Class 2 Opp'n at 5; Joint Creators Class 4 Opp'n at 3 (noting that proponents only provided "brief and vague descriptions of some projects operated by 'youth media educators' without identifying any actual uses of audiovisual works protected by access controls").

[372] Joint Creators Class 3 Opp'n at 3; DVD CCA/AACS LA Class 4 Opp'n at 5-7; Joint Creators Class 4 Opp'n at 3.

[373] Joint Creators Class 1 Opp'n at 3.

[374] Joint Creators Class 4 Opp'n at 5-6 (urging the Register to "consider how the DMCA and access controls have supported a vast increase in the public's access to works when considering the propriety of any exemption that applies to everyone even tangentially associated with any non-profit organization").

Beyond these general arguments raised by opponents with respect to all of the proposed audiovisual classes, they offer the following specific arguments concerning the individual proposed classes.

a. Proposed Class 1: Colleges and Universities

Opponents do not object to renewing the current exemption for colleges and universities, which permits faculty and students to circumvent access controls to obtain short portions of works on DVDs and material obtained online for purposes of criticism and comment in film studies and similar courses requiring close analysis of motion picture excerpts. But they oppose expanding the exemption to encompass all educational uses or to AACS-protected Blu-ray discs, relying on the general arguments described above.[375] In particular, they argue that proponents have not demonstrated that alternatives to accessing Blu-ray are insufficient. They also maintain that the current regulatory language limiting circumvention to uses of short portions of motion pictures for purposes of criticism and comment serves a valuable purpose in curbing abuse and protecting the integrity of the relevant access controls.[376]

b. Proposed Class 2: Primary and Secondary Schools (K-12)

Opponents DVD CCA and Joint Creators do not object to renewing the current exemption permitting K-12 teachers to circumvent access controls to obtain short portions of works on DVDs and online material for purposes of criticism and comment in film studies and similar courses requiring close analysis of motion picture excerpts. But they oppose extending the exemption to cover educational uses in general or uses by K-12 students (as opposed to their teachers).[377]

DVD CCA and AACS LA contend that the examples provided of K-12 student video projects do not demonstrate adverse effects due to the prohibition on circumvention but instead "demonstrate that students are successfully making use of copyrighted works."[378] In addition, opponents dispute that diminished student pride should be considered an adverse effect "when high quality video and images could have been obtained through video capture software from DVD playback."[379] Moreover, Joint

[375] AACS LA Class 1 Opp'n at 2-5; DVD CCA Class 1 Opp'n at 2-3; Joint Creators Class 1 Opp'n at 2-3.

[376] *See, e.g.*, Joint Creators Class 1 Opp'n at 4-5.

[377] DVD CCA Class 2 Opp'n at 2; Joint Creators Class 2 Opp'n at 2; Tr. at 197:05-13 (May 27, 2015) (Williams, Joint Creators); Tr. at 203:23-204:02 (May 27, 2015) (Williams, Joint Creators) ("[W]e are troubled by the idea of introducing very young children, in some instances, to circumvention technologies that can certainly be misused and we're afraid would be misused.").

[378] AACS LA Class 2 Opp'n at 8; DVD CCA Class 2 Opp'n at 8.

[379] AACS LA Class 2 Opp'n at 8 (using the terms "video capture" and "screen capture" interchangeably); DVD CCA Class 2 Opp'n at 8; *see also* Joint Creators Class 2 Opp'n at 5-6 (noting that a diminished sense of pride and "a feeling that 'education is not valued in their society . . . . does not establish that preserving the contours of the current exemptions would result in any substantial adverse effects on the ability of educators or students to make noninfringing uses of audiovisual works").

Creators found other examples of student-created projects on University of Notre Dame's "Remix T" website cited by proponents, such as a "lip dub" of the trailer for the film *Inception*, troublesome because "re-creating the voiceover and music of a commercial film trailer is questionable as a fair use."[380] They also fear that allowing circumvention by students "would indicate to students that hacking access controls is acceptable as long as they use the material in school."[381]

AACS LA objects to extending an exemption to AACS-protected Blu-ray discs, even if restricted to uses by educators, noting that proponents introduced no evidence of specific "AACS-protected works as an example of the use they desire to make."[382] AACS LA points out that Hobbs' sole example, of a teacher wanting to use Blu-ray clips from a Shakespeare movie, was undermined by her admission that DVDs could be successfully employed to achieve the desired use.[383]

Finally, in response to Hobbs' concerns over the cost of various methods suggested as alternatives to circumvention, Joint Creators assert that cost is not an adverse effect "even remotely caused by access controls."[384] They further contend that the cost of using licensed materials is overstated by proponents.[385]

c. Proposed Class 3: Massive Open Online Courses (MOOCs)

All opponents oppose granting any exemption for MOOCs, at least as the exemption was originally proposed.[386] They argue that the uses are unlikely to be noninfringing fair uses, because "the major providers of MOOCs are for-profit."[387] Joint Creators assert that the effect of such uses on the market for copyrighted works would be "much greater than in a traditional, limited classroom setting, as the courses would be

[380] Joint Creators Class 2 Opp'n at 4.

[381] *Id.*

[382] AACS LA Class 2 Opp'n at 2, 7-8; *see also* Joint Creators Class 2 Opp'n at 5; Tr. at 191:02-09 (May 27, 2015) (Turnbull, AACS LA).

[383] AACS LA Class 2 Opp'n at 4; *see also id.* at 8 (student uses of YouTube videos does not demonstrate need for high-definition qualify).

[384] Joint Creators Class 2 Opp'n at 6.

[385] Joint Creators emphasize that proponents inflate the costs of at least one of the services available for these uses, Discovery Education, asserting that instead of costing more than $10,000 or more per annual subscription (as claimed by proponents), this source costs "only $1,600 per year/per building, for K-8 schools, and $2,150 per year/per building for high schools." *Id.*

[386] DVD CCA/AACS LA Class 3 Opp'n at 3; Joint Creators Class 3 Opp'n at 2. DVD CCA/AACS LA and Joint Creators note that they may not be opposed to a narrowly tailored exemption that fits within the constraints of the TEACH Act. Tr. at 126:17-127:02 (May 27, 2015) (Turnbull, DVD CCA/AACS LA); Tr. at 130:12-17 (May 27, 2015) (Williams, Joint Creators).

[387] DVD CCA/AACS LA Class 3 Opp'n at 7-8 (citing *Princeton Univ. Press v. Mich. Document Servs.* , 99 F.3d 1381 and *Cambridge*, 769 F.3d 1232); Joint Creators Class 3 Opp'n at 4.

distributed broadly over the internet."[388] Joint Creators suggest the "broad definition of MOOC" makes it difficult to assess whether uses are likely noninfringing.[389]

DVD CCA/AACS LA also contend that the activities of MOOCs are unlikely to qualify as noninfringing under the TEACH Act, codified as section 110(2) of title 17.[390] They note that educational institutions engaging in distance learning under the TEACH Act must be nonprofit and accredited, whereas "many, and perhaps most, MOOCs are offered by institutions that do not satisfy these requirements."[391] Opponents point out that even where MOOC providers partner with accredited institutions, such as Harvard, University of Maryland, or Duke, enrollment is not limited to matriculated students, and assert that this undermines the TEACH Act's enrollment requirement.[392] DVD CCA/AACS LA also assert that the legislative history of the TEACH Act demonstrates congressional intent that the nonprofit, accredited institution and enrollment requirements operate as safeguards against unauthorized dissemination of materials over the internet.[393] DVD CCA/AACS LA note that the major MOOC platforms, Coursera, EdX, and Udacity, generally do not employ TPMs on their online courses, and so do not satisfy section 110(2)'s requirement to employ technological measures to restrict transmissions only to those authorized to receive them.[394] They further suggest, however, that these platforms have a number of options to apply TPMs to course materials if they so choose.[395] Joint Creators also posit that some uses could fall under the existing

[388] Joint Creators Class 3 Opp'n at 4.

[389] *Id.* at 5; *see also* Tr. at 120:01-04 (May 27, 2015) (Turnbull, DVD CCA/AACS LA). DVD CCA/AACS LA express concern that it is unclear who would be liable should there be infringement, particularly as between an affiliated institution and a MOOC provider. Tr. at 142:03-143:02 (May 27, 2015) (Turnbull, DVD CCA/AACS LA).

[390] DVD CCA/AACS LA Class 3 Opp'n at 4.

[391] *Id.* at 5 (noting "two of the largest MOOC providers, Coursera, which accounts for more than one-third of all MOOCs offered in 2014, and Khan Academy, are for-profit entities"); *see also* Joint Creators Class 3 Opp'n at 5-6 (claiming the TEACH Act "is not relevant . . . because 'it is limited to systematic instruction as part of a curriculum of an accredited, non-profit institution,' while MOOCs are open to anyone"); Tr. at 127:12-16 (May 27, 2015) (Turnbull, DVD CCA/AACS LA).

[392] DVD CCA/AACS LA Class 3 Opp'n at 5; Joint Creators Class 3 Opp'n at 5-6 (stating "becoming a 'student' in a MOOC, and potentially eligible for the exemption, is as easy as directing one's [i]nternet browser to any given MOOC"); *see also* Tr. at 119:23-25 (May 27, 2015) (Turnbull, DVD CCA/AACS LA).

[393] DVD CCA/AACS LA Class 3 Opp'n at 6.

[394] AACS LA/DVD CCA Class 3 Post-Hearing Resp. at 2; DVD CCA/AACS LA Class 3 Opp'n at 5-6; *see also* Tr. at 122:01-05 (May 27, 2015) (Turnbull, DVD CCA/AACS LA).

[395] AACS LA/DVD CCA Class 3 Post-Hearing Resp. at 2-5 (citing MediaCAST, Chegg and Vital Source Bookshelf e-reader platforms, Apple's FairPlay technology, DRMtoday, EZDRM.com, Expressplay.com, aBuyDRM.com, and Verimatrix.com as examples of TPM services for various online platforms); *see also* Joint Creators Class 3 Post-Hearing Resp. (deferring to AACS LA/DVD CCA on these questions).

exemption for noncommercial videos, thus rendering a separate exemption for MOOCs unnecessary.[396]

In addition to these concerns, opponents urge that Joint Educators have failed to demonstrate adverse effects.[397] Joint Creators state that Joint Educators' assertion that "online students are more easily distracted than students in the classroom, and have much lower course completion rates," is not an adverse effect resulting from access controls, but rather "is endemic to the nature of MOOCs, which have notoriously low student retention rates."[398] DVD CCA/AACS LA points out that MOOCs have grown over the past ten years without an exemption, and suggest that any slowed growth is a result of "other concerns about the long-term viability and sustainability of MOOCs as a pedagogical model."[399] Joint Creators further observe that proponents did not provide sufficient examples that students enrolled in MOOCs were adversely affected by the current prohibition.[400]

Looking to the statutory factors, Joint Creators conclude that the "sheer numbers and the very nature of MOOCs as 'massive' counsel against adoption of this exemption,"[401] and that "the open and unregulated nature of the MOOC industry makes it difficult to define a properly tailored exemption . . . that does not run the risk of opening up motion pictures to widespread hacking by anyone claiming to participate in a MOOC."[402]

d. Proposed Class 4: Educational Programs Operated by Museums, Libraries or Nonprofits

Opponents uniformly oppose granting a broad exemption for educational uses by museums, libraries or nonprofits.[403] They nonetheless indicate that they may be amenable to a limited exemption "more in the character of the existing educational exemptions."[404] According to DVD CCA/AACS LA, the proposed exemption for

---

[396] Joint Creators Class 3 Opp'n at 8 n.23 (referencing Professor Decherney's planned course on Hollywood).

[397] DVD CCA/AACS LA Class 3 Opp'n at 8.

[398] Joint Creators Class 3 Opp'n at 6-7; *see also* Tr. at 131:21-25 (May 27, 2015) (Williams, Joint Creators) (positing that the dearth of motion picture clips in online courses may have more to do with practical concerns rather than the inability to circumvent protected works).

[399] DVD CCA/AACS LA Class 3 Opp'n at 10.

[400] Joint Creators Class 3 Opp'n at 7-8 (noting that the only example provided by proponents was "a video essay assignment that Professor Peter Decherney plans to offer on the Hollywood film industry").

[401] *Id.* at 2.

[402] *Id.* at 9.

[403] DVD CCA/AACS LA Class 4 Opp'n at 3; Joint Creators Class 4 Opp'n at 2.

[404] Tr. at 245:10-246:22 (May 27, 2015) (Smith, USCO; Turnbull, DVD CCA/AACS LA); *see also id.* at 250:18-25 (Williams, Joint Creators).

"programs operated by museums, libraries or nonprofits" defines "an unreasonably large, unworkable class."[405] Joint Creators voice concerns that this language would "open[] up this proposed exemption to a number of organizations that may have no connection to education," since not all nonprofit organizations have "educational missions."[406]

DVD CCA/AACS LA contends that proponents did not clearly identify the particular uses they would like to make of protected works, rendering it "impossible to know whether [the] proposed . . . activities 'for education purposes' would be noninfringing."[407] They also fault proponents' use of undefined terms such as "digital media and learning," "educators," and "learners" in describing the scope of the proposed exemption, noting that the term "learners" in particular is so vague that "no determination could ever be assured that such uses would be educational at all."[408]

In addition, DVD CCA/AACS LA assert that any remote or online activities proposed by proponents as part of this class would "likely fall outside the bounds of the TEACH Act," and so would not be noninfringing.[409] First, the proposed exemption not only includes museums and libraries that are not necessarily nonprofit, but also "omits any requirement that [institutions] must be accredited."[410] Second, it is "unclear" whether the users of the exemption would satisfy the TEACH Act's enrollment requirement.[411] Third, DVD CCA/AACS LA assert that the legislative history of the TEACH Act "instructs that transmissions containing copyrighted works only be made to those identified persons authorized to receive them, either by password-protected website accounts or other technological means," and proponents have not addressed these requirements.[412]

DVD CCA/AACS LA maintain that proponents have not demonstrated adverse effects, but made only "very generalized statements about the value of 'learners' being able to 'learn how to create and express themselves using digital media tools.'"[413] They

---

[405] DVD CCA/AACS LA Class 4 Opp'n at 3; *see also* Joint Creators Class 4 Opp'n at 4; Tr. at 244:10-19 (May 27, 2015) (Turnbull, DVD CCA/AACS LA) (stating "the categories that are suggested here are very vague and very broad"); Tr. at 248:25-249:12 (May 27, 2015) (Williams, Joint Creators).

[406] Joint Creators Class 4 Opp'n at 4; *see also* Tr. at 244:11-18, 245:05-09 (May 27, 2015) (Turnbull, DVD CCA/AACS LA).

[407] DVD CCA/AACS LA Class 4 Opp'n at 5.

[408] *Id.* at 5-6; *see also* Joint Creators Class 4 Opp'n at 3-4. "Learners" are defined as those who "come to the library to 'hang out, mess around and geek out' and learn how to create and express themselves using digital media tools, including music, video and multimedia." DVD CCA/AACS LA Class 4 Opp'n at 5.

[409] DVD CCA/AACS LA Class 4 Opp'n at 3, 6-7.

[410] *Id.* at 6.

[411] *Id.* at 7.

[412] *Id.*; Tr. at 247:25-248:11 (May 27, 2015) (Turnbull, DVD CCA/AACS LA).

[413] DVD CCA/AACS LA Class 4 Opp'n at 8 (citing Hobbs Class 4 Supp. at 2); *see also* Joint Creators Class 4 Opp'n at 5 (asserting that proponents "have failed to provide any concrete examples of the uses

also argue that proponents did not provide examples of "specific works that a would-be beneficiary of the proposed exemption seeks to use [on DVDs] but has been unable to do so," and did not explain a need for Blu-ray material or high-definition video.[414]

e. Proposed Class 5: Multimedia E-Books

Opponents do not object to renewing the current exemption for multimedia-e-books, which permits circumvention of access controls to obtain short portions of works on DVDs and material obtained online for purposes of criticism and comment in nonfiction multimedia e-books offering film analysis. All opponents oppose expanding the current exemption to allow circumvention of AACS on Blu-ray discs, to remove the limitation to uses for purposes of film analysis, criticism and comment, or to remove the limitation to uses of short portions of works.[415] In addition to the general arguments above, AACS LA and DVD CCA contend that because proponents of Class 5 have not identified specific examples of other fair uses in the context of multimedia e-books, an exemption cannot be granted for this "much broader scope requested by proponents."[416] Instead, they claim that proponents' examples are limited to uses involving film analysis, such as exploring the use of sound in film.[417] Joint Creators further note that no examples have been presented to support "expansion of the exemption to [include uses for purposes of] fictional authorship."[418]

On adverse effects, opponents assert that proponents have not demonstrated that Blu-ray content is necessary for their uses, with Joint Creators pointing out that many of proponents' examples "refer to material that is not exclusively available on Blu-ray Discs."[419] AACS LA and DVD CCA also assert that screen-capture software is especially appropriate for e-books because it offers "highly suitable" resolution and "can be used with e-book authors' preferred software, *Adobe InDesign*," which has the ability to embed video files, such as mpeg-2 and mpeg-4 files, in e-books.[420]

---

they seek to enable" and thusly have failed to show adverse effects caused by the prohibition on circumvention).

[414] DVD CCA/AACS LA Class 4 Opp'n at 8.

[415] Joint Creators Class 5 Opp'n at 2; AACS LA Class 5 Opp'n at 2; DVD CCA Class 5 Opp'n at 2; Tr. at 88:20-89:04 (May 28, 2015) (Williams, Joint Creators).

[416] AACS LA Class 5 Opp'n at 6; DVD CCA Class 5 Opp'n at 6; *see also* Joint Creators Class 5 Opp'n at 3-4.

[417] AACS LA Class 5 Opp'n at 6; DVD CCA Class 5 Opp'n at 5-6; *see also* Joint Creators Class 5 Opp'n at 3.

[418] Tr. at 89:13-22 (May 28, 2015) (Williams, Joint Creators).

[419] Joint Creators Class 5 Opp'n at 4-6; *see also* AACS LA Class 5 Opp'n at 2-3, 6-9; DVD CCA Class 5 Opp'n at 6-8; Tr. at 80:02-05 (May 28, 2015) (Turnbull, AACS LA); Tr. at 92:11-19 (May 28, 2015) (Williams, Joint Creators).

[420] AACS LA Class 5 Opp'n at 11-13; *see also* DVD CCA Class 5 Opp'n at 9-11; AACS LA Class 5 Opp'n at Exhibit 2; Tr. at 83:04-84:12, Exhibits 23-24 (May 28, 2015) (Taylor, DVD CCA) (demonstrating how to add clips in Adobe InDesign and compilation of clips taken from James Bond movies using *Camtasia*).

f. Proposed Class 6: Filmmaking Uses

Opponents do not object to renewing the current exemption for filmmaking uses, which permits circumvention of access controls to obtain short portions of works on DVDs and material obtained online for purposes of criticism and comment in documentary films. Opponents, however, oppose extending the exemption to allow circumvention of AACS on Blu-ray discs, to cover narrative (*i.e.*, fictional) films, to permit use of more than short portions of motion pictures, or to permit uses beyond criticism and comment.[421] In addition to the general arguments above, opponents argue specifically that "even when a second work exhibits some transformative characteristics from the underlying work, the new work will infringe if it takes an unnecessary amount, slavishly copies from the original, or the purpose of the secondary work is no different than that of the original."[422] They contend that "the industry, at least in regard to biopic films, is succeeding in the marketplace" despite access controls.[423] Joint Creators assert that proponents did not define "specific parameters within which fictional filmmakers should operate to restrain the scope of the [proposed] exemption."[424] AACS LA and DVD CCA also contend that the record does not include a sufficient number of uses in fictional films to permit a determination that such uses are likely to be noninfringing.[425] Finally, they argue that "fair use does not compel a copyright holder to hand over a copy of the work so that fair use can be made," arguing that licensing is appropriate rather than circumventing TPMs.[426]

AACS LA and Joint Educators also contend that proponents did not establish that high-definition or Blu-ray-quality images are necessary for distribution, suggesting that film festivals and distributors such as PBS "do not appear to have clear policies to exclude a film . . . because it contains a clip that is not of the same quality of the overall film."[427] Opponents do not, however, contend that screen-capture software would be

---

However, DVD CCA concedes that clips taken from DVDs using screen capture software would not be "DVD quality" because the DVDs themselves are not perfect, asserting instead that the "images are of sufficient quality" for proponents' uses. Tr. at 84:16-24 (May 28, 2015) (Taylor, DVD CCA).

[421] AACS LA Class 6 Opp'n at 2; DVD CCA Class 6 Opp'n at 2; Joint Creators Class 6 Opp'n at 2; *see also* Tr. at 60:17-61:03 (May 20, 2015) (Williams, Joint Creators).

[422] AACS LA Class 6 Opp'n at 6-7 (citing *Castle Rock Entm't v. Carol Publ'g*, 150 F.3d 132 (2d Cir. 1998) and *Warner Bros. Entm't, Inc. and J. K. Rowling v. RDR Books*, 575 F. Supp. 2d 513 (S.D.N.Y. 2008)); DVD CCA Class 6 Opp'n at 5-6 (citing same); *see also* Tr. at 62:04-19 (May 20, 2015) (Williams, Joint Creators).

[423] AACS LA Class 6 Opp'n at 16-17 (discussing *Selma* and other examples raised by Joint Filmmakers); DVD CCA Class 6 Opp'n at 14-15; *see also* Tr. at 66:12-67:08 (May 20, 2015) (Williams, Joint Creators).

[424] Joint Creators Class 6 Opp'n at 3-4; *see also* 61:04-15 (May 20, 2015) (Williams, Joint Creators).

[425] AACS LA Class 6 Opp'n at 7-9; DVD CCA Class 6 Opp'n at 6-8.

[426] AACS LA Class 6 Opp'n at 12-13; DVD CCA Class 6 Opp'n at 10-11.

[427] AACS LA Class 6 Opp'n at 17-19; Joint Creators Class 6 Opp'n at 5-6 (stating that PBS' Editorial Standards and Policies include film quality as only one of many factors considered by the broadcaster).

acceptable to these distributors.[428] Rather, they suggest that upconverting lower-resolution DVD to HD quality would be "acceptable within [PBS'] definition of HD," a solution that Joint Filmmakers reject, as explained above.[429]

Opponents further maintain that expansion of the exemption is not warranted under the statutory factors. Under the first factor, Joint Creators assert that access controls have increased the availability of copyrighted works.[430] Under the fourth factor, proponents, including Simon Swart of Twentieth Century Fox, contend that an exemption would negatively impact a currently vibrant clip-licensing market.[431] DVD CCA urges the Librarian to consider as an additional "other factor" under the statutory test the need to "curb the abuse of the exemption," as allegedly demonstrated in examples provided by proponents indicating uses of higher-quality images that were not necessary to engage in criticism and comment of the underlying work.[432]

g. Proposed Class 7: Noncommercial Videos

Opponents do not object to renewing the current exemption permitting circumvention of access controls to obtain short portions of works on DVDs, as well as material obtained online, for purposes of criticism and comment in noncommercial videos. But Joint Creators oppose any expansion of the current exemption, including to anything more than "short" portions, to uses beyond "noncommercial" works, or by removing the limitation that uses be for purpose of criticism and comment.[433] In addition, opponents express an overarching concern that many such videos are not necessarily fair uses, with AACS LA arguing that "the vast majority of remix videos cannot be defended under the fair use doctrine."[434]

Contending that screen-capture software is sufficient for purposes of remixing high-definition source material, AACS LA and DVD CCA submitted duplicate exhibits which attempted to recreate the *Take It Away* video by covering the Washington Redskins' logo on a football helmet with a bright orange dot, allegedly resulting in the "same effect" as NCAI's original video.[435] EFF/OTW point out in reply comments, however, that this screen-captured version was of a lower resolution than the original,

[428] Tr. at 19:17-24 (May 20, 2015) (Smith, USCO; Taylor, DVD CCA).

[429] *Id.* at 94:02-12 (Turnbull, AACS LA; Charlesworth, USCO).

[430] Joint Creators Class 6 Opp'n at 6.

[431] Tr. at 79:23-80:01 (May 20, 2015) (Swart, Twentieth Century Fox Home Entertainment; Charlesworth, USCO).

[432] DVD CCA Class 6 Opp'n at 20-22; *see also* Tr. at 20:07-21:09 (May 20, 2015) (Taylor, DVD CCA).

[433] Joint Creators Class 7 Opp'n at 4.

[434] AACS LA Class 7 Opp'n at 3-8; DVD CCA Class 7 Opp'n at 6; Joint Creators Class 7 Opp'n at 3 (analyzing *SupreMacy*); Joint Creators Class 7 Post-Hearing Resp. at 3 (analyzing *Worthy* vid submitted during hearing); *but see* Tr. at 295:10-11 (May 28, 2015) (Williams, Joint Creators) (admitting "we're not claiming that there aren't a significant number of fair uses").

[435] AACS LA Class 7 Opp'n at 10, Exhibit 1; DVD CCA Class 7 Opp'n at 10, Exhibit 1.

thus obviating the need to obscure the logo on other players' helmets, the turf, and fan apparel.[436]

Finally, no opponents expressed a position concerning whether the much-discussed screen-capture technologies also required circumvention within the meaning of section 1201, with Joint Creators noting they had not "independently tested" the technologies.[437]

3. Discussion

The current proposals describe an array of uses of proposed motion picture excerpts that proponents contend are non-infringing and are likely to be adversely affected in the next three years by section 1201(a)(1)'s prohibition on circumvention of TPMs. While the proposed uses are more specifically discussed on a class-by-class basis below, the record reveals certain commonalities.

First, the Register concludes that any exemption should be limited to uses of "motion pictures," as opposed to the broader category of "audiovisual works." Under section 101 of the Copyright Act, "motion pictures" are a broad subset of "audiovisual works" that includes television shows, online videos, news, commercials, and other works consisting of a "series of related images which, when shown in succession, impart an impression of motion, together with accompanying sounds, if any."[438] While EFF/OTW agreed with the "motion pictures" limitation so long as the breadth of this phrase could be made clear to non-lawyer users,[439] others sought an exemption for audiovisual works generally.[440] But the record demonstrates insufficient need to circumvent TPMs on audiovisual works that are not "motion pictures." While Joint Educators contend that video game excerpts can be used in classroom instruction, it is unclear how or why circumvention of TPMs would be necessary to incorporate a video game excerpt as a pedagogical tool, as opposed to showing a filmed clip of game play (for example, from Twitch or YouTube). Similarly, while Joint Filmmakers referenced an abandoned planned documentary utilizing clips from video games, again there was no record provided to support the necessity for or specifics of any circumvention activities to obtain the clips.[441] Accordingly, as no further examples of non-motion-picture

[436] EFF/OTW Reply at 11.

[437] Joint Creators Class 7 Post-Hearing Resp. at 3; *see also* AACS LA/DVD CCA Class 7 Post-Hearing Resp.

[438] 17 U.S.C. § 101; *see also* 1-2 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 2.09 (2015) ("1-2 NIMMER ON COPYRIGHT"). Video games are copyrightable and may be registered by the Copyright Office as computer programs, literary works, or as audiovisual works, but are not typically registered as motion pictures. *See* 1-2 NIMMER ON COPYRIGHT § 2.09; *Atari Games Corp. v. Oman*, 888 F.2d 878 (9th Cir. 1989); *Midway Mfg. Co. v. Artic Int'l, Inc.*¸ 704 F.2d 1009 (7th Cir. 1983).

[439] EFF/OTW Supp. at 22 (agreeing with "motion picture" limitation).

[440] *See* Joint Educators Class 1 Supp. at 10 (seeking expansion to include video games); Hobbs Class 2 Supp. at 1; Hobbs Class 4 Supp. at 1.

[441] Tr. at 109:14-110:15 (May 20, 2015) (Quinn, Kartemquin Educational Films; Charlesworth, USCO).

audiovisual works were provided to support a broader exemption, the Register declines to recommend an exemption for excerpts of "audiovisual works," as opposed to "motion pictures."

Second, these requested exemptions implicate the same types of TPMs regardless of proposed non-infringing use. As explained above, proponents each seek an exemption that would apply to CSS-protected DVDs, AACS-protected Blu-ray discs, and various TPMs applicable to online distribution services. The record in this proceeding again confirms that CSS is a technological measure that controls access to motion pictures on DVDs, and that AACS is a measure that controls access to motion pictures on Blu-ray discs.[442] Proponents also assert that various technologies that protect motion pictures available via online streaming and digital download services constitute access controls within the meaning of section 1201(a)(1).[443] Opponents do not appear to disagree,[444] instead observing that "these access controls have increased the availability of works and have allowed for a vast proliferation of platforms" for consumers to enjoy authorized content.[445] In light of this record, the Register concludes that a significant number of platforms that offer digitally transmitted motion pictures, both for digital downloads and for streaming, constitute technological measures controlling access to those works under section 1201(a)(1).

Third, and as further discussed below, based on the record submitted regarding non-infringing uses of material distributed over streaming media services, the Register agrees with Joint Creators' suggestion to replace the current phrase "online distribution services" with the phrase "digitally transmitted video" to more appropriately describe the media that proponents seek to use. Indeed, the parties understand the current exemption to encompass both streamed and downloaded content.[446] Additionally, as discussed below, the exemptions would retain the qualifications that uses be limited to "short portions" of motion pictures and for enumerated purposes related to criticism and commentary.[447]

---

[442] *See* Joint Filmmakers Supp. at 3, App. J; EFF/OTW Supp. at 2; *see also* 2012 Recommendation at 126.

[443] *See, e.g.*, Joint Filmmakers Supp. at 3, App. J; EFF/OTW Supp. at 2 (collectively referencing RTMPE, SWF, Fair Play, HTML5 and planned encryption of standard).

[444] *See, e.g.*, Joint Creators Class 7 Opp'n at 2-3 (referencing EFF/OTW's description of online access controls); Joint Creators Class 6 Opp'n at 2; *but see* Joint Creators Class 1 Opp'n at 3 n.4 (stating that Joint Educators had not established that streaming platforms use access controls to intentionally block access to works on projectors).

[445] *See, e.g.*, Joint Creators Class 6 Opp'n at 2; Joint Creators Class 7 Opp'n at 2-3; Joint Creators Class 1 Opp'n at 3.

[446] Tr. at 306:17-308:01 (May 28, 2015) (Williams, Joint Creators; Smith, USCO); *see also* 37 C.F.R. § 201.40(b)(4)-(7).

[447] *See* Tr. at 307:07-308:01 (May 28, 2015) (Williams, Joint Creators) (supporting revision but seeking clarification that librarying would remain prohibited).

a. Noninfringing Uses

Proponents of the various classes all claim that a significant number of the proposed uses of motion pictures fall within the favored purposes of criticism and commentary referenced in the preamble of section 107 and are therefore likely to be fair uses.[448] For example, Professor Decherney uses motion picture excerpts as part of a course he teaches on the history of Hollywood, and NCAI has used footage of a Washington Redskins football game to demonstrate its position that seeing the team's name and logo are not required to enjoy watching the game. Accordingly, the Register proceeds to consider the four-factor test set out in section 107.

While otherwise analyzing each class of proposed uses separately, the Register notes that factors two and three remain relatively constant across the proposed uses. Under factor two, it is well established that motion pictures are generally creative and thus at the core of copyright's protective purposes.[449] But for transformative uses, the second factor may be of relatively limited assistance to evaluate whether a use is fair.[450] As in 2012, the Register concludes that the second fair use factor slightly disfavors the proposed exemptions, but is not especially relevant to most of the proposed uses.[451]

Under the third factor, the Register again concludes that the limitation to circumvention for uses of "short portions" of motion pictures is integral to the various proposals.[452] Some proponents contested the necessity of this limitation, contending that a use should be judged by whether or not it is proportionate to the intended transformative goals, and that numerical limits specifying the appropriate amount of a work that may be used are inappropriate.[453] But while recognizing that the extent of permissible copying may vary,[454] the Register suggests that the "short portions" limitation provides useful guidance as to what is generally likely to be a fair use in these contexts without imposing a wholly inflexible rule as to length.[455] As a general matter, longer uses are less likely to be considered fair because they are more likely to usurp the market for a work. At any rate, the record provides few if any examples where the use of

---

[448] *See* 17 U.S.C. § 107.

[449] In 2012, the Register also noted that while the assessment of the actual nature of a copyrighted work will vary from case to case, the record generally revealed examples of motion pictures that were more creative, rather than factual. *See* 2012 Recommendation at 128. The same is true for this rulemaking.

[450] *Campbell*, 510 U.S. at 586.

[451] *See* 2012 Recommendation at 128.

[452] *See id.*

[453] *See, e.g.*, Joint Educators Class 1 Reply at 8 (citing *Cambridge*, 769 F.3d 1232); Hobbs Class 4 Reply at 6 (same); Joint Filmmakers Supp. at 19-20; Tr. at 9:02-05 (May 27, 2015) (Butler, Joint Educators).

[454] *Campbell*, 510 U.S. at 586.

[455] *See, e.g.*, Tr. at 102:20-105:20 (May 20, 2015) (Charlesworth, USCO; Quinn, Kartemquin Educational Films); Tr. at 89:05-11 (May 28, 2015) (Williams, Joint Creators) (stating "the short portions limitation, for example, really keeps this closer to what is very likely to be fair use, and so we think it's important to retain those types of limitations").

a "longer" clip was necessary,[456] and indeed, submissions from proponents of exemptions for noncommercial videos, MOOCs, and use in e-books suggest that the formats themselves dictate that clips be brief.[457] While hypotheticals were raised concerning the use of multiple short clips from the same motion picture—and whether such multiple uses would qualify for the exemption—the Register notes that the limitation to "short portions" does not categorically exclude them. The critical question is whether, in the aggregate, such uses would be noninfringing.

i. Proposed Class 1: Colleges and Universities

Joint Educators demonstrated that a significant number of the proposed uses are for purposes of criticism and commentary, which are favored uses under the preamble of section 107 and therefore likely to be fair. Analyzing the first factor, Joint Educators introduced multiple examples of uses for commentary, criticism, scholarship and teaching in a nonprofit educational context that appeared to represent transformative uses of the original work.[458] These included, for example, an instructor's use of short video clips to provide context for ethnomusicology lectures, or a student's completion of a video essay project that required the use of still images and video for a cinema studies course.[459]

As explained above, the second and third factors are neutral or tend to favor proponents. Looking to the fourth factor, when the use of a work is for criticism or commentary or otherwise transformative, it is presumed to be less likely to compete with the market for the underlying work. Notably, opponents do not contest that the brief, educationally oriented uses in this proposed class are likely to be fair uses; nor have they introduced evidence that the intended uses by faculty and students are likely to undermine the value of copyright-protected motion pictures.[460]

Accordingly, while the Register makes no judgment as to whether any particular uses submitted by Class 1 proponents (or by proponents of the other audiovisual classes) are in fact fair, the record demonstrates that many of the uses suggested by proponents appear likely to be fair and thus to qualify as a noninfringing purpose under section 107.

---

[456] Tr. at 13:08-19:24 (May 27, 2015) (Smith, USCO; Butler, Joint Educators); *id.* at 64:24-65:10 (Williams, Joint Creators) (noting that Joint Creators did not challenge whether alleged use of "longer excerpts" fell outside exemption).

[457] *See* EFF/OTW Supp. at 15; Joint Educators Class 3 Supp. at 10; *see also* EFF/OTW Supp. at 22 ("We do not oppose language of this sort, providing that it can be made clear that 'short' has no specific definition outside a comparison to the particular works at issue and the remixer's needs."); Joint Educators Class 1 Supp. at 23 (requesting limitation that was limited to use of "short portions" of motion pictures); Tr. at 106:19-20 (May 20, 2015) (Lerner, Joint Filmmakers) (noting "we don't disagree with what you said about [short portions] not being a bright line rule"); Tr. at 105:03-04 (May 20, 2015) (Quinn, Kartemquin Educational Films) (agreeing "in most cases, the term 'short' is sufficiently vague").

[458] *See* Joint Educators Class 1 Reply at 4-6; Joint Educators Class 1 Supp. at 7; Sheff Supp. at 1.

[459] *See* Joint Educators Class 1 Supp. at 7; Joint Educators Class 1 Reply at 20.

[460] *See, e.g.*, Joint Creators Class 1 Opp'n; DVD CCA Class 1 Opp'n.

ii. Proposed Class 2: Primary and Secondary Schools (K-12)

Similarly, Class 2 proponents demonstrated that a significant number of the proposed uses within primary and secondary schools—for example, comparing the depiction of the 1920s in the film *Chicago* with the book *The Great Gatsby*[461]—are likely to be non-infringing fair uses under section 107, and opponents do not contest this aspect of the petition. Because the purpose and character of the uses are for criticism and comment and also within a nonprofit educational setting, the first factor favors fair use.[462] As explained above, the second and third factors are neutral or tend to favor proponents. Finally, the Register agrees that the brief and transformative nature of these educational uses makes them unlikely to interfere with the markets for the underlying works.[463]

While the record is relatively light on whether standard definition or higher-quality resolution is required to make the proposed uses of the material, as discussed further below, it does suggest that a significant number of the proposed uses are likely to be fair and would qualify as noninfringing under section 107.

iii. Proposed Class 3: Massive Open Online Courses (MOOCs)

Analysis of this proposed exemption for faculty and students participating in MOOCs must first grapple with varying attempts to define its contours. Class 3 proponents initially took the position that it would be inappropriate to limit the types of programs qualifying for an exemption, for example, by imposing standards for user registration or terms of use, or distinguishing between nonprofit or commercial initiatives.[464]

While acknowledging the organic and rapid growth of programs understood to be MOOCs since the last rulemaking, the Office shares AACS LA's concern that an "unbounded exemption" where "[a]nybody can declare that they're teaching a MOOC" and "anyone can be a student" is anathema to the exemption process as envisioned by Congress.[465] That said, the record contains specific examples of uses proposed by proponents, and suggests that proponents' focus is on a more circumscribed category of offerings made available by universities, such as Professor Decherney's proposed MOOC titled *The Hollywood Film Industry*, or HarvardX's interdisciplinary series of courses

[461] Hobbs Class 2 Supp. at 4.

[462] *Id.* at 4-5.

[463] *Id.* at 3, 9.

[464] Proponents explain that some MOOCs do not require registration, that "[b]y definition, MOOCs are free to participate in," and that Coursera and Udacity, two of the major MOOC platforms, are for-profit entities. Joint Educators Class 3 Supp. at 5-6 & n.15 (citing *Harvard Open Courses: Open Learning Initiative*, HARVARD EXTENSION SCHOOL, http://www.extension.harvard.edu/open-learning-initiative ("You do not need to register to view the lecture videos.")).

[465] Tr. at 119:18-121:16 (May 27, 2015) (Turnbull, DVD CCA/AACS LA); *see id.* at 129:03-130:24 (Williams, Joint Creators).

titled *ChinaX*.[466] Professor Decherney explained that platforms like Coursera or Udacity do not themselves offer courses, but rather are used by universities or other organizations to distribute the online courses that the institutions have created.[467] Opponents, for their part, expressed significantly greater comfort if this proposed class were to be limited to courses offered by accredited institutions such as colleges and universities.[468]

Against this backdrop, the Register must consider whether the specific proposed uses are likely to be non-infringing under section 110(2), or under section 107 as fair uses. While the record is not as well developed as it might be, it appears that some universities perhaps have relied upon section 110(2) in offering live synchronous online courses that are limited by registration and size.[469] But the parties seem to agree that many MOOCs, as commonly understood, are likely to fall out of bounds of the TEACH Act for one or more reasons.[470]

The Register acknowledges proponents' hesitation to claim that the proposed uses meet the TEACH Act's requirement that all uses are made "under the actual supervision of an instructor as an integral part of a class session offered as a regular part of the systematic mediated instructional activities of . . . an accredited non-profit educational institution."[471] The legislative history indicates that the phrase "systematic mediated instructional activities" was intended to encompass uses of works in ways "analogous to live-classroom lectures,"[472] and the record disclosed no judicial interpretation to flesh out how analogous they must be. The Register recognizes that while to some degree they may mimic a traditional classroom setting, MOOCs are typically structured differently than live-classroom lectures (*e.g.*, lessons can be completed on-demand, are offered on a standalone basis, and are shorter than traditional live-classroom lectures). In certain

[466] Joint Educators Class 3 Supp. at 8, 12.

[467] Tr. at 134:07-137:16 (May 27, 2015) (Decherney, Joint Educators; Charlesworth, USCO).

[468] *See, e.g.*, *id.* at 142:03-143:02 (Turnbull, DVD CCA/AACS LA).

[469] *See, e.g.*, *id.* at 145:19-149:07 (Decherney, Joint Educators; Charlesworth, USCO).

[470] *Id.* at 98:03-06 (Butler, Joint Educators); *id.* at 127:04-19 (Turnbull, DVD CCA/AACS LA).

[471] *See* 17 U.S.C. § 110(2)(A); *see also id.* § 110(11) (defining " mediated instructional activities" as "activities that use such work as an integral part of the class experience, controlled by or under the actual supervision of the instructor and analogous to the type of performance or display that would take place in a live classroom setting. The term does not refer to activities that use, in 1 or more class sessions of a single course, such works as textbooks, course packs, or other material in any media, copies or phonorecords of which are typically purchased or acquired by the students in higher education for their independent use and retention or are typically purchased or acquired for elementary and secondary students for their possession and independent use").

[472] The legislative history suggests that the congressional motivation was to exclude uses of works which students would typically be required to purchase as part of a coursepack as opposed to viewed in a live lecture. *See* S. REP. NO. 107-31, at 9-10 (2001) (noting the phrase is "intended to require the performance or display to be analogous to the type of performance or display that would take place in a live classroom setting").

cases, MOOCs may qualify for the exception under section 110(2). But the record also suggests that in other cases, they may not.

It appears that many existing MOOCs may not meet section 110(2)'s standards by choice rather than by inherent design. MOOCs may lack a formalized enrollment process,[473] fail to institute policies or provide notices to students regarding copyright,[474] or lack the types of protections against unauthorized redistribution of copyrighted content that Congress envisioned in enacting that section.[475] In the case of enrollment policies, the Register notes that edX, a major MOOC platform, does impose enrollment requirements on students. Section 110(2)(D)(ii) of the TEACH Act requires transmitting bodies or institutions to implement technological measures that "reasonably prevent retention of a work in accessible form . . . for longer than the class session; and unauthorized further dissemination of the work in accessible form."[476] While AACS LA and others contend that it would not be "particularly burdensome" for platforms to implement TPMs on streamed or downloaded content—and indeed the extensive record submitted in connection with various requests to circumvent TPMs on digitally distributed material supports this suggestion[477]—Joint Educators claim that implementing TPMs of the kind required by section 110(2) "would be an unwelcome and unnatural fit for most MOOC providers."[478]

While the TEACH Act may not itself provide a comprehensive basis for a finding of noninfringing use in the MOOC context, the Register believes that the Act, which became law in 2002, provides useful and important guidance as to Congress' intentions regarding the need for and nature of excepted uses to permit certain performances and displays of copyrighted works for distance learning. As discussed below, the Register recommends that any exemption for uses in connection with MOOCs be tied to key aspects of section 110(2), including its emphasis on implementation of TPMs in distance learning that incorporates copyrighted works.

Turning to the alternative noninfringing basis of fair use, the record primarily contains examples of MOOCs that are provided by accredited nonprofit educational

[473] *See* 17 U.S.C. § 110(2)(C).

[474] *See id.* § 110(2)(D)(i).

[475] H.R. REP. NO. 107-687, at 11-13 (2002).

[476] *See* 17 U.S.C. § 110(2)(D)(ii) (also requiring that transmitting bodies or institutions do not interfere with TPMs used by copyright owners to prevent such retention or unauthorized further distribution).

[477] Tr. at 122:22-123:16 (May 27, 2015) (Turnbull, DVD CCA/AACS LA); *see also, e.g.*, AACS LA/DVD CCA Class 3 Post-Hearing Resp. at 2-5 (citing MediaCAST, Chegg and Vital Source Bookshelf e-reader platforms, Apple's FairPlay technology, DRMtoday, EZDRM.com, Expressplay.com, aBuyDRM.com, and Verimatrix.com as examples of TPM services for various online platforms).

[478] Band/Butler/Decherney Class 3 Post-Hearing Resp. at 2.

institutions (albeit sometimes through third-party platforms) and it is these types of uses that the Register will proceed to analyze under the four-factor test.[479]

First, Joint Educators demonstrated that a significant number of the planned uses by faculty reproduce portions of motion pictures for purposes of criticism and commentary, favored purposes in the preamble of section 107. For example, Professor Decherney plans to offer a MOOC titled *The Hollywood Film Industry* that is similar to classroom and live synchronous online courses he has previously offered to students enrolled at the University of Pennsylvania.[480] Other examples included an interdisciplinary course on Chinese history and culture and the study of German cinema.[481] Moreover, because the examples provided concerned courses offered by universities operating on a nonprofit basis,[482] this further favors proponents. Without suggesting that a court would find each and every one of the proposed uses to be transformative or otherwise favored under the factor first, the record nonetheless indicates that a significant number be viewed positively under this factor.

As discussed above, while the second fair use factor does not favor an exemption, it is not especially relevant here. Turning to the third factor, especially in light of the fact that MOOC segments tend to be at most ten minutes in length for all of the content presented, the proposed uses of excerpts of motion pictures within these segments are likely to be brief as well. This factor therefore favors proponents.

Finally, as to the fourth factor, uses of modest amounts of motion pictures in a transformative manner for purposes of criticism or comment are less likely to interfere with the primary or derivative markets for the motion picture.[483] Opponents have not demonstrated that the specific examples provided by proponents would diminish the value of copyright-protected works.[484]

---

[479] While Butler noted that some MOOC offerers are nonprofits but not "accredited institutions," including Khan Academy, the World Bank, and National Geographic Society, proponents did not introduce specific evidence that these nonprofits are seeking to benefit from the proposed exemption. *Compare* Tr. at 118:05-118:23 (May 27, 2015) (Butler, Joint Educators), *with* 17 U.S.C. § 110(2).

[480] *See* Joint Educators Class 3 Supp. at 8-9; Tr. at 145:19-149:07 (May 27, 2015) (Decherney, Joint Educators; Charlesworth, USCO) (describing similarities and differences between non-MOOC online, live synchronous courses and Professor Decherney's planned MOOC); *see also* Tr. at 145:02-09 (May 27, 2015) (Butler, Joint Educators) (describing proposed MOOC about German films).

[481] *See, e.g.*, Joint Educators Class 3 Supp. at 4-5, 12 (referencing courses in computer science, business, engineering, art and design, health and medicine and describing a *China* course offered by HarvardX); Joint Educators Class 3 Reply at 10-11 (referencing proposed MOOC on German "Lola" award-winning films).

[482] *See* Joint Educators Class 3 Reply at 10-11; *see also* Joint Educators Class 3 Supp. at 4-5, 8, 12.

[483] *See* 2012 Recommendation at 129; *Campbell*, 510 U.S. at 591-92.

[484] The market for works protected by access controls is addressed below in the context of the 1201 statutory factors.

On balance, and without passing judgment on any particular use described by proponents, the fair use analysis indicates that a substantial number of the proposed uses of motion picture excerpts for criticism and comment in MOOCs offered by nonprofit educational institutions are likely to qualify as noninfringing under section 107. Some may also qualify as excepted uses under section 110(2).[485]

iv. Proposed Class 4: Educational Programs Operated by Museums, Libraries or Nonprofits

Much of the discussion surrounding the proposed exemption for museums, libraries and nonprofits concerned the appropriate contours of such a class. For example, Hobbs was persuasive on the point that an organization accredited to confer GEDs should be treated similarly to a K-12 school.[486] But the language proposed in her petition was far broader and would seemingly encompass over 1.5 million nonprofit organizations in the United States, regardless of purpose or mission statement.[487] In reply comments, Hobbs suggested the exemption could be limited to "digital and media literacy instructional practices in informal learning contexts."[488] Accordingly, the Register limits the following analysis to these types of digital and media literacy programs.

While Hobbs references a large number of library, museums, and other organizations, and describes a handful of media literacy programs, including after-school programs, the record is short on specific proposed noninfringing uses of copyrighted material. The examples provided were limited to GED-conferring and adult education programs using short portions of motion pictures for purposes of criticism and commentary in the course of face-to-face instruction. Specifically, an instructor proposes to have her students incorporate motion picture excerpts into poetry video essays as part of a GED program, and a nonprofit media literacy organization proposes to circumvent TPMs on the television series *Orange is the New Black* so that program participants can comment upon the portrayal of African-American women in the series.[489] These sorts of uses are favored in the preamble of section 107 and likely to be transformative under the first fair use factor. As explained above, the second and third fair use factors are neutral or tend to favor proponents. In analyzing the fourth fair use factor, as with the other

[485] In reaching this conclusion, the Register notes that section 110 shall not "be construed to imply further rights under section 106 of this title, or to have any effect on the defenses or limitations on rights granted under any other section of [] title [17]." 17 U.S.C. § 110(11).

[486] Hobbs Class 4 Reply at 5; Tr. at 231:09-232:08 (May 27, 2015) (Hobbs).

[487] *See* Joint Creators Class 4 Opp'n at 4 n.4 (noting that the National Center for Charitable Statistics lists over 1.5 million registered nonprofit organizations in the United States). Nor was the original proposal limited to 501(c)(3) organizations; it also encompassed, for example, political organizations structured under 501(c)(4), professional football leagues structured under 501(c)(6), and cemetery companies organized under 501(c)(13).

[488] Hobbs Class 4 Reply at 5.

[489] *See* Hobbs Class 4 Supp. at 4; Hobbs Class 4 Reply at 5, 8; Tr. at 231:09-232:08, 234:11-235:25, 258:14-259:08 (May 27, 2015) (Hobbs).

educational classes, the Register agrees that the types of transformative uses of brief clips that proponents are suggesting are unlikely to interfere with the markets for the underlying copyrighted works.

Accordingly, while the Register makes no judgment as to whether any particular uses submitted by Class 4 proponents are in fact fair,[490] it appears that many of the proposed uses would likely be considered fair and noninfringing under section 107.

v. Proposed Class 5: Multimedia E-Books

Although in the case of multimedia e-books the record with respect to proposed uses was leaner than in some other classes, the Register finds that Class 5 proponents have sufficiently demonstrated that some meaningful portion of the proffered uses are likely to be fair. For example, proponents seek to incorporate motion picture excerpts in e-books analyzing techniques in motion picture sound editing or cinematography.

First, the record includes examples of prospective e-books in which filmmakers, cinema studies professors, and other authors seek to conduct close analysis of and provide commentary on short excerpts of motion pictures.[491] At least at the present time, the technical limitations of the medium (*i.e.*, maximum file sizes) will seemingly limit the uses of the excerpted works to relatively brief segments. Although many of these e-books may be commercial endeavors, because the excerpts are used for the purposes of criticism and commentary, they may well be productive and transformative uses.[492] That said, the Register nonetheless agrees with opponents that the record lacks evidence demonstrating a need to expand the current exemption to include uses in fictional e-books or for purposes beyond close analysis of the underlying work, as no examples of such uses were submitted.

As with the other classes, the second and third factors are less relevant. But under the fourth factor, the brevity and transformative nature of the proposed uses favors an exemption because the proposed users are unlikely to substitute for the original work—and indeed opponents did not identify any proposed use that has in the past harmed, or is likely in the future to harm, the market for or value of any copyrighted motion pictures.[493]

---

[490] As noted above, the record was limited to examples of uses in GED-conferring programs or adult education programs, and proponents stipulated that they did not seek an exemption for uses that would fall outside "digital and media literacy instructional practices in informal learning contexts." The Register therefore declines to analyze other theoretical uses, such as exhibitions or public presentations before general audiences in libraries or museums.

[491] *See* Authors Alliance Supp. at 11-13; Tr. at 95:12-24 (May 28, 2015) (Williams, Joint Creators).

[492] *See* 2012 Recommendation at 128 (citing *Campbell*, 510 U.S. at 583-85).

[493] *Campbell*, 510 U.S. at 591-92.

Accordingly, again without opining on the fairness of any particular proposed use, the Register concludes that the record demonstrates that many of the contemplated uses are likely to be noninfringing under section 107.

vi. Proposed Class 6: Filmmaking Uses

Joint Filmmakers introduced numerous examples of uses of short excerpts of motion pictures in documentary films to provide criticism, commentary, or educate, which the Register agrees may represent "paradigmatic fair uses of copyrighted works."[494] These include: a documentary of the life of former U.S. Attorney General Ramsey Clark (featuring news clips of Clark),[495] the documentary *Inequality for All* (using clips to illustrate America's widening income gap),[496] and *These Amazing Shadows* (telling the story of the history and importance of the National Film Registry).[497] No commenters dispute the validity of such uses by documentary filmmakers. Obtaining quality motion picture source material can be vital to illustrate context for public debate, examine history and popular culture, and otherwise further documentary storytelling.[498] As the Register has concluded in prior rulemakings, because documentaries use motion picture clips to provide commentary and/or criticism—and often, invaluable insight into the subject matter of the film—such uses are likely to be transformative and are favored under the preamble of section 107. This can be true even when a film is intended for commercial release.[499]

Considering the statutory fair use factors, first, as explained, the use in documentaries is likely to be transformative in nature; second, while motion pictures are generally creative in nature, this is less true in the case of archival news footage and, at any rate, this factor is neutralized by the transformative proposed uses in documentaries; third, proponents seek to use quantitatively small portions of excerpts, favoring fair use; and fourth, use of a motion picture clip for purposes of documentary commentary or criticism is unlikely to interfere with the primary or derivative markets for the underlying work. Accordingly, the Register again concludes that many of the proposed uses in documentary filmmaking are likely to be non-infringing fair uses.

The thornier question for this rulemaking is whether proponents have demonstrated that uses beyond documentary filmmaking—alternatively described by commenters as "narrative," "fictional" or "scripted" filmmaking, or in terms of narrower subsets such as "biopics" or films "based on a true story"—are likely to be fair. Joint

---

[494] *See* Joint Filmmakers Supp. at 5, Apps. D-G, App. I; *see also id.* at App. L (listing 23 events held by organizations to inform filmmakers about guidelines for fair use in filmmaking).

[495] *Id.* at 9.

[496] *Id.* at 13.

[497] *Id.* at 17.

[498] *See, e.g.*, *id.* at App. D (Letter from Kenn Rabin).

[499] *See* 17 U.S.C. § 107; 2012 Recommendation at 127-29; 2010 Recommendation at 49-52.

Filmmakers point to many examples of uses of motion picture excerpts in non-documentary films, such as a scripted biopic of civil rights leader Cesar Chavez (using news clips),[500] Oliver Stone's forthcoming "take on the Edward Snowden saga" (using news clips),[501] and a fictional film that "explores what it would be like for a 70s black family watching *Roots*" (showing clips from *Roots*).[502] The Register proceeds to evaluate whether the current record adequately supports the contention that the proposed uses of motion picture excerpts within various types of non-documentary films are likely to be non-infringing.[503]

At the outset, the use of motion picture clips in narrative films diverges from educational uses and uses in documentaries because there is no presumption that their primary purpose is to offer criticism or commentary, as opposed to being included for entertainment purposes.[504] Previously granted exemptions have been limited to uses of motion picture excerpts for purposes of criticism and comment—that is, purposes explicitly identified by Congress as fair uses in the preamble to section 107.[505] To be sure, it may be possible for narrative films to use motion picture clips for purposes of criticism or comment, or for uses of motion picture clips for purposes other than criticism and comment to be fair uses. The Register acknowledges proponents' view that some fictional filmmaking may offer criticism and commentary through "techniques such as parody, reference, and pastiche" or "present information and commentary meant to educate and analyze real events."[506] But with narrative films there is a significant countervailing concern: that copyrighted works will be used in a manner that may supplant the existing, robust licensing market for motion picture clips.[507] This might be true, for example, when a clip is simply used to move a fictional or quasi-fictional storyline forward.[508] To support their proposal for a broader exemption, Joint

[500] *See* Joint Filmmakers Supp. at App. G (Letter from Pablo Cruz).

[501] *See id.* at App. C at Chart 1.

[502] *See id.* at App. C at Chart 2; *see also id.* at App. I at 9 (statement of Matt Latham) (referencing a planned narrative film "that satirizes the representation of women in cinema"); *id.* at App. M (Letter of Adam Folk) (describing the narrative film *Welcome to New York* which incorporated news coverage of Dominique Strauss-Kahn in an allegedly transformative manner); Lerner et al. Post Hearing Resp. at 2-3 (describing the narrative film *Experimenter* which portrays the life of psychologist Stanley Milgram and uses clips from the television show *Candid Camera* to draw parallels between the show and social psychology; further describing transformative nature of Strauss-Kahn footage).

[503] In 2012, the Register concluded that the record presented lacked "concrete examples" that would allow her to conduct an adequate fair use analysis with respect to fictional films. 2012 Recommendation at 130.

[504] *See id.* Of course, the Register recognizes that many documentaries are highly entertaining, and does not suggest that entertaining works cannot also make transformative use of preexisting material. Instead, the Register means only to differentiate uses which are not intended to offer commentary.

[505] *See* 17 U.S.C. § 107; 2010 Final Rule, 75 Fed. Reg. at 43,827; 2012 Final Rule, 77 Fed. Reg. at 65,266.

[506] Joint Filmmakers Supp. at 5.

[507] *See* Tr. at 79:08-14 (May 20, 2015) (Swart, Twentieth Century Fox Home Entertainment) ("We actually do a pretty vibrant licensing business.").

[508] *See* 2012 Recommendation at 130.

Filmmakers submit testimony from non-documentary filmmakers[509] as well as a list of more than 30 narrative films that were awarded errors and omissions ("E&O") insurance coverage since the 2012 rulemaking notwithstanding the use of unlicensed material, or where certain uses of unlicensed material was deemed a fair use by a court.[510] While this list may provide additional context, the Register must perform her own analysis. In particular, the issuance of E&O insurance—which provides coverage in the event of a lawsuit for copyright infringement, among other things—is not equivalent to a determination of fair use, but only a representation that an underwriter agrees to insure the film against any prospective claim. Similarly, none of the case law examples provided by proponents considered the use of motion picture excerpts in narrative films, but rather involved reenactments, quotations, filming of fine art, or other types of uses.

In considering the factual record, the Register considered whether there might be an appropriate way to limit the types of narrative films to which the exemption might conceivably apply, so as to permit a more limited set of uses while minimizing the potential impact upon legitimate licensing of the underlying works. Of the uses of motion picture clips set forth by proponent Michael Donaldson in the list of films obtaining E&O insurance, the overwhelming majority were classified as "based on a true story" or "biopics."[511] The Office thus specifically invited participants, after the public hearings, to provide information describing any commonly accepted differences between documentary, biopics, and other categories of films.[512] But the responses revealed less than complete agreement as to the meaning of the term "documentary," let alone categories such as "documentary-like," "biopic," "docudrama," "based on a true story," "films that portray real events," "inspired by," "imaginative," or "totally fiction."[513] Accordingly, the Register is unable on this record to draw sound distinctions among different types of narrative films. Moreover, the parties did seem to agree that it would be inappropriate to grant an exemption for some types of non-documentary films but not others—with, of course, proponents favoring a full exemption and opponents favoring none whatsoever. In analyzing the fair use question for use of clips in non-documentary

[509] Joint Filmmakers Supp. at App. D (Letter from Kenn Rabin), App. F (Letter from Michael Mailer), App. G (Letter from Pablo Cruz), App. H (Letter from Finite Films), App. I (Filmmaker Testimony), App. M (Letter of Adam Folk).

[510] *Id.* at App. C (Letter from Michael Donaldson).

[511] *Id.*

[512] *See* Post-Hearing Questions to Class 6 Witnesses (June 3, 2015).

[513] *See* NMR Post Hearing Resp. at 2-3 (noting that "filmmakers across genres of filmmaking borrow many techniques and conventions from each other," and citing professor of film studies Cy Kuckenbaker when noting that accepted documentaries like *Exit Through the Gift Shop* and *The Act of Killing* "consciously subvert traditional assumptions about genre and their relation to fact and fiction"); *see generally* Class 6 Post-Hearing Responses.

films, the Register is therefore unable, on this record, to restrict her analysis to any predetermined subsets of films.[514]

With respect to non-documentary films, the first statutory factor, the purpose and character of the use, does not clearly favor proponents. While the purpose of this rulemaking is not to opine on specific uses, the Register observes that, based on the record in this proceeding, a number of examples of uses offered by proponents do not necessarily appear to be related to criticism or comment or otherwise transformative. For example, the description of the film *Mandorla* offered by Joint Filmmakers suggests that multiple excerpts from the film *Excalibur* are perhaps being used to flesh out the motivations of the main character and further the storyline, and it is not immediately apparent that these uses are transformative or should not be licensed.[515] Similarly, proponents reference *Farah Goes Bang*, a film about a "woman in her twenties who tries to lose her virginity while campaigning across America for presidential candidate John Kerry in 2004."[516] Because the campaign clips may be used for entertainment purposes, it is not clear that the uses are transformative. Joint Filmmakers also point to uses of motion picture excerpts in scripted films such as *Selma* or *Good Night and Good Luck*, but it appears that in those cases, the uses were licensed.[517]

As explained above, the second factor, the nature of the work, tends to weigh against a finding of fair use because motion pictures are generally creative. As with the other proposed classes, the third factor tends to favor proponents because presumably the uses would be limited to short portions of the overall work.

Considering the fourth factor, the effect of the use on the potential market for or value of the copyrighted work, the record suggests that extending an exemption to narrative films may interfere with primary or derivative markets for the underlying work and, in particular, the licensing market for motion picture excerpts. Joint Filmmakers suggest that limiting the exemption to uses of short portions of clips makes it unlikely that the proposed uses will interfere with the market for the underlying copyrighted work as a whole,[518] but this does not address the effect on the licensing market for the clips themselves. While Joint Filmmakers profess to "have no interest in an exemption that

[514] To the extent relevant in a future rulemaking, the Register would welcome additional filmic examples or written analysis of an appropriate way to describe a specific category of narrative films that are more likely to make noninfringing use of motion picture excerpts.

[515] *Mandorla* is described as a movie about "[a] man with an over active imagination. It calls him away from the realities of corporate and family life to face a dark and magical place in a medieval French city." It apparently uses "[c]lips from Excalibur which constantly makes him want to recreate the scene in his own life." Joint Filmmakers Supp. at App. C at Chart 2; *see also* Tr. at 62:11-19 (May 20, 2015) (Williams, Joint Creators) (discussing need for licensing of uses of excerpts to "grab the audience's attention").

[516] Joint Filmmakers Supp. at App. C at Chart 2.

[517] *See id.* at 18; *id.* at App. D (Letter from Kenn Rabin) (discussing obtaining licenses for both uses).

[518] Joint Filmmakers Reply at 6.

covers clips just for entertainment value,"[519] proponents offer no satisfying way to refine this category to exclude "entertainment value" uses from the types of transformative uses associated with documentary filmmaking. Meanwhile, opponents raise persuasive concerns that an exemption for non-documentary films would undermine a vibrant licensing market.[520] The fourth factor therefore weighs relatively substantially against fair use.

On balance, the fair use analysis reveals that while a significant number of the proposed documentary uses would qualify as noninfringing under section 107, as framed by proponents and based on the record provided, the Register cannot conclude that the suggested non-documentary uses are likely to be noninfringing.

vii. Proposed Class 7: Noncommercial Videos

As in previous rulemakings, the Register finds that Class 7 proponents have demonstrated that a significant number of the proposed uses to create noncommercial videos involve criticism and commentary, which are privileged uses under section 107.[521] More specifically, turning to the first fair use factor, the Register has previously observed that noncommercial videos may take clips from motion pictures to make a point about the underlying works and/or to convey a political message, and the evidence submitted in this proceeding includes many examples of videos that illustrate such uses, such as NCAI's *Take It Away* video,[522] video lectures providing in-depth film criticism,[523] and a remix video calling attention to sexism in a famous game show.[524] In many instances, then, the first fair use factor weighs in favor of proponents.

That said, the record is not uniform in this regard. The Register credits opponents' concern that several of the videos provided as examples may be insufficiently transformative to support a determination of fair use.[525] While understanding that familiarity with the original material and the "vidding" genre may sometimes be required to fully appreciate the transformative aspects of certain remix videos,[526] it is not clear that various "trailer-style" videos submitted in connection with this proposed class—often

[519] Tr. at 42:05-43:01 (May 20, 2015) (Lerner, Joint Filmmakers).

[520] *See id.* at 79:23-80:01 (Swart, Twentieth Century Fox Home Entertainment).

[521] *See* Joint Creators Class 7 Opp'n at 3 (acknowledging that "noncommercial video creators often make fair uses of materials from other motion pictures"); DVD CCA Class 7 Opp'n at 4 (accord).

[522] *See* NCAI Supp. at 1.

[523] *See* EFF/OTW Supp. at App. A at 4 (referencing Tony Zhou's *Every Frame a Painting* video series).

[524] *See id.* at App. A at 3 (referencing *The Price is Creepy* vid); *see also generally* EFF/OTW Reply at 17, App. A; EFF/OTW Supp. at Apps. A, Q.

[525] *See, e.g.*, DVD CCA Class 7 Opp'n at 5-6 (citing *Warner Bros. v. RDR Books*, 575 F. Supp. 2d 513); AACS LA Class 7 Opp'n at 5-8 (same).

[526] *Compare* EFF/OTW Reply at 3-4, App. A (discussing *SupreMacy* vid), *with* Joint Creators Class 7 Opp'n at 3-4.

consisting of a montage of scenes from a specific movie or television show accompanied by a preexisting soundtrack from another source—sufficiently "change[] the meaning or message" of the underlying work to be considered transformative.[527] Nor does the case law provided by EFF/OTW support the view that montages and like uses that appear to offer mainly entertainment rather than commentary are inherently transformative; such uses may instead be derivative works that require permission from the copyright owners of the original work. The Register emphasizes that limiting the scope to uses of motion pictures for purposes of criticism or commentary is integral to fashioning an appropriate exemption for this class.

Because the second and third factors are neutral or favor proponents, as explained above, the analysis next turns to the fourth factor, the effect upon the market for the copyrighted work. As explained in the 2012 rulemaking, when the proposed uses are transformative, it is less likely that there will be interference with the primary or derivative markets for the underlying work.[528] The Register additionally notes that there is no record evidence that an appropriately crafted exemption will harm the market for copyrighted works. Indeed, EFF/OTW offered some evidence that the owners of the underlying works may appreciate the attention that fan remix videos bring to the original work.[529]

Accordingly, without opining on whether any particular use is in fact fair or not fair, the Register concludes that the record demonstrates that a substantial number, though not all, of the proffered uses are likely to be noninfringing under section 107.

b. Adverse Effects

Proponents have established that certain noninfringing uses contemplated by Proposed Classes 1 through 7 can be achieved if circumvention is allowed, but this does not end the inquiry. The Register must also determine whether the prohibition on circumvention is causing adverse effects, including whether it is possible that proponents may make these noninfringing uses without circumventing access controls.

At the outset, the Register concludes that generally speaking, copyrighted motion pictures are not widely available in formats not subject to technological protections.[530] While the record shows that the various formats considered in this rulemaking—DVD,

---

[527] EFF/OTW Supp. at 6. *See* Joint Creators Class 7 Post-Hearing Resp. at 3 (discussing *Worthy* vid creator's statement that the music was selected because "it sounded similar to what was used in the show"); *see also* Joint Creators Class 7 Opp'n at 3-4; DVD CCA Class 7 Opp'n at 5-6; AACS LA Class 7 Opp'n at 5-8.

[528] 2012 Recommendation at 129.

[529] *See* EFF/OTW Reply at 6 n.14. For example, the *Worthy* video when viewed on YouTube was paired with an advertisement from WarnerBros Television to "Watch this show" for a fee. Volta1228, *Worthy (Supernatural – Dean / Mark of Cain Vid)*, YOUTUBE, https://www.youtube.com/watch?v=tcC01yJivmU (last visited Oct. 7, 2015) (cited in Joint Creators Class 7 Post-Hearing Resp. at 3).

[530] For example, no commenters suggested that VHS or 35mm were viable alternatives.

Blu-ray, and digitally transmitted video—may sometimes constitute alternatives to one another, the record also indicates that each of these formats is typically protected by access controls.

i. General Viability of Alternatives to Circumvention

Next, the Register evaluates the various alternatives opponents suggest are viable alternatives to circumvention, namely, licensing, smartphone and camera video recording, screen-capture applications, and services that provide online access to materials otherwise available in physical formats, including digital rights libraries and "disc-to-digital" services.

The record clearly demonstrates that licensing of motion picture clips is not a viable alternative for the uses proposed for criticism and comment.[531] The content available for clip licensing is far from complete and in any event such licensing is not practicable in many cases, whether due to difficulties in locating the rightsholders, overly lengthy negotiations that preclude planned uses, or denials where the would-be licensor disapproves of the noninfringing use.[532] Furthermore, requiring a creator who is making fair use of a work to obtain a license is in tension with the Supreme Court's holding that rightsholders do not have an exclusive right to markets for criticism or comment of their copyrighted works.[533]

Unlike in previous rulemakings, opponents do not appear to take the position that smartphone recording provides an adequate substitute for circumvention in most or all cases.[534] But they suggest that smartphone recording is an acceptable alternative for Proposed Class 3 specifically, concerning uses in MOOCs, or more generally across the proposed classes, to obtain access to Blu-ray exclusive footage.[535] Proponents generally object that such recordings yield significantly inferior audio and video quality, and no exhibits were offered to establish the contrary.[536] For their part, Joint Educators argue that the MOOC experience demands equal, or potentially higher, content resolution than uses in live classrooms.[537] While concerns specific to Blu-ray are discussed further

[531] As explained above, the licensing market may operate more effectively for uses for entertainment purposes.

[532] *See, e.g.*, Joint Educators Class 1 Supp. at 21; Hobbs Class 2 Supp. at 7; Joint Filmmakers Supp. at 11-13; EFF/OTW Supp. at 6.

[533] *Campbell*, 510 U.S. 569.

[534] *See* 2012 Recommendation at 131-32.

[535] *See* DVD CCA/AACS LA Class 3 Opp'n at 13-14; Joint Creators Class 3 Opp'n at 8; AACS LA Class 1 Opp'n at 14 (suggesting smartphone or professional camera recordings are viable alternatives for Blu-ray content); AACS LA Class 2 Opp'n at 13 (same); DVD CCA/AACS LA Class 4 Opp'n at 13 (same); AACS LA Class 5 Opp'n at 12-13; AACS LA Class 6 Opp'n at 21; AACS LA Class 7 Opp'n at 11, 16 (same).

[536] For example, Morrissette of Kartemquin Educational Films states that the resulting quality is degraded so significantly as to be unusable for film distribution purposes. *See* Joint Filmmakers Supp. at App. B.

[537] Joint Educators Class 3 Supp. at 10-11.

below, the Register finds that the record does not establish that smartphone recordings can serve as sufficient alternatives to circumvention.

Whether various screen-capture technologies can function as adequate alternatives for DVD content or online material was more hotly contested across these classes. Notably, AACS LA does not maintain that screen capture of the playback of a Blu-ray produces video of comparable image quality to Blu-ray itself, but does contend the screen-capture technologies are much improved since the last rulemaking cycle and are thus suitable for certain purposes.[538] The record contains many examples of screen-capture technologies, most of which are available for less than $100, and in some cases, for free.[539] The record also demonstrates that these products can be relatively easy to use and are generally able effectively to capture content played back from DVDs, Blu-ray discs, and online streaming services.[540] Finally, the record also suggests that a variety of screen-capture technologies are available for use on either Windows or Apple operating software, although the makers of some of these programs suggest that use of the software may itself require circumvention, particularly on a Mac.[541]

Proponents offered extensive commentary and evidence to rebut arguments that screen-captured images are sufficient for their needs.[542] Based on the video evidence, hearing testimony and written submissions offered by both parties, the Register concludes that while screen-capture technology has improved markedly since the last rulemaking, and may satisfy some purposes, overall, screen-captured images still remain of lower quality than those available via circumvention of access controls on motion pictures. The question remains whether screen-capture applications are acceptable for the proposed uses.

Notably, for Proposed Class 6, DVD CCA concedes that screen-capture software would not be acceptable for Joint Filmmakers' distribution needs, and Joint Filmmakers have documented examples where distribution quality standards preclude the use of screen-captured footage.[543] The Register finds Joint Filmmaker's evidence persuasive

[538] Tr. at 45:01-05 (May 27, 2015) (Turnbull, AACS LA; Smith, USCO); Tr. at 264:01-09 (May 28, 2015) (Turnbull, AACS LA)*; see also, e.g.*, DVD CCA Class 7 Opp'n at 10-14.

[539] *See generally* DVD CCA Opp'n for Classes 1-7.

[540] Tr. at 62:13-63:07 (May 27, 2015) (Taylor, DVD CCA) (describing how WM Capture technology "is very straightforward and fairly intuitive"); *see also, e.g.*, DVD CCA Class 1 Opp'n at 8; DVD CCA Class 2 Opp'n at 8-9; DVD CCA/AACS LA Class 4 Opp'n at 10; *but see* Hobbs Class 4 Reply at 7-8.

[541] *See, e.g.*, AACS/DVD CCA Class 1 Post-Hearing Resp.; Band/Butler/Decherney Class 1 Post-Hearing Resp. at 2; Benmark et al. Class 3 Post-Hearing Resp. at 2.

[542] In addition to the video exhibits, the Register found the statements from Professor Tisha Turk and Kartemquin Educational Films' Jim Morrissette, each providing detailed technical analysis, particularly helpful. *See* EFF/OTW Supp. at App. N; Joint Filmmakers Supp. at App. B; *see also, e.g.*, EFF/OTW Reply at 11-16; EFF/OTW Post-Hearing Resp. (analyzing insufficiency of exhibits provided by DVD CCA).

[543] *See* Tr. at 19:17-24 (May 20, 2015) (Smith, USCO; Taylor, DVD CCA); *id.* at 9:20-10:13, 98:20-10:09 (Morrissette, Kartemquin Educational Films); Joint Filmmakers Supp. at Apps. B, D, I.

and concludes that the inability to obtain higher-quality footage through circumvention has adverse effects on filmmakers as a result of current distribution standards.

The record also supports the conclusion that screen-capture technology is at times inadequate for other types of uses as well. While screen-capture technology has improved, the record generally demonstrates that consumer devices and expectations have at the same time increased as high definition continues to supplant standarddefinition and ultra-high-definition formats (*i.e.*, 4K and 8K resolution) begin to penetrate the market. For example, Class 7 proponents EFF/OTW and NCAI provided video evidence and commentary indicating that screen-capture technology was insufficient to communicate as effective a message about the Redskins logo, as the original *Take It Away* video relied on circumvention of high-definition material.[544] Based on this evidence, the Register is able to perceive that *Take It Away* would suffer due to loss of detail in depicting the Redskins logo in its various manifestations if the video could only be made with screen-captured images.

But the record does not demonstrate that all noncommercial videos covered by Proposed Class 7 require high-quality images that would be obtained through circumvention of access controls on DVDs, Blu-ray discs, or digitally transmitted video.[545] For example, EFF/OTW submitted "mash-up" videos that mix images from one source with audio from another,[546] and other videos that simply add subtitles over material from a single source.[547] Because these examples do not obviously require high quality source material to serve their objectives, it is not apparent that screen-capture technology would not be a suitable alternative.

The Register also finds substantial evidence on this record to support a finding that e-book authors under Proposed Class 5 are likely to suffer adverse effects if they are unable to incorporate higher than screen-capture quality material in cases where the ability to convey a point depends upon perception of details or subtleties in a motion picture excerpt.[548] This was illustrated in a representative proposed use submitted by Academy-Award winning sound editor Mark Berger, who wishes to make an e-book entitled *Listening to Movies* that explores how uses of sound relate to a film's moving images; Berger explained that the compression required to convert material into a lower-resolution format results in unwanted artifacts that distort the audio track.[549]

---

[544] *See* NCAI Supp. at 1; EFF/OTW Supp. at 9.

[545] *See* 2012 Recommendation at 134.

[546] EFF/OTW Supp. at App. A at 1 (citing *Avatar/Pocahontas Mashup*); *see id.* at App. A at 2 (citing *The Rent is Too Damn UP*). Proponents also cite a *Ferris Bueller* remix which falls into a similar category. *Id.* at App. A at 1 (citing *Ferris Bueller* Remix).

[547] *See id.* at App. A at 1, 2-3 (citing The Master and St01en Collective's *Lord of the Rings*).

[548] *See, e.g.*, Authors Alliance at 11 (regarding sound editing); *id.* at 13 (regarding use of color in the film *The Godfather*).

[549] *Id.* at 11.

Similarly, the record supports a finding that some number of educational uses by faculty and students at colleges and universities under Proposed Class 1, by nonprofit educational institutions offering MOOCs under Proposed Class 3, as well as by K-12 educators covered by Proposed Class 2—including those teaching GED courses—may depend upon close analysis of images that would be adversely affected if students cannot apprehend the subtle detail of the analyzed images. Proponents offer a variety of examples to support this point, such as the inability of screen-capture technology to capture a dissolve between a Soviet girl standing in a harvest field and her body lying on the ground, to convey natural details in the documentary *Planet Earth*,[550] or to portray subtle details in a classic film such as *Citizen Kane*.[551] In contrast to these examples, where precise detail is not required for the use in question, for example, to illustrate a general historical point, provide cultural or historical context, or add visual interest to a lecture or page of text,[552] screen-captured images may be fully adequate to fulfill the noninfringing use.

With respect to K-12 *students* covered by Proposed Class 2, on the present record, the Register concludes that screen-capture technology is a viable alternative to circumvention for those students' educational needs. While the record supports the potential need for K-12 educators to access higher-quality content—for example, to present film analysis or engage in close study of natural phenomena—there was virtually no evidence to suggest that students had the same educational need.[553] Rather, it appears that K-12 student uses—such as providing a factual report on McDonald's founder Roy Kroc or overlaying students' own spoken narrative on top of music videos—do not typically depend upon close analysis and can be achieved through the use of screen-capture tools.[554] Although the Register is sympathetic to Hobbs' argument that K-12 students should not be precluded from engaging in the same types of film-related educational activities as university students, the current record does not offer evidence that K-12 students engage in equivalent uses. Moreover, while Hobbs claims that screen-capture technology can be expensive or difficult to use, as explained above, the Register finds that to the contrary, the record demonstrates that easy, low-to-no-cost options are available. If there is continuing desire to extend this exemption to students, the Register is hopeful that a more robust record will be submitted in the next rulemaking.[555]

---

[550] Joint Educators Class 1 Supp. at 14, 18 (referencing *Planet Earth* and *The Soviet Story*).

[551] Hobbs Class 2 Supp. at 5.

[552] Joint Educators Class 1 Supp. at 7, 9.

[553] *See, e.g.*, Hobbs Class 2 Supp. at 5 (discussing use of excerpts from *Citizen Kane* and *The Patriot*).

[554] *See, e.g.*, Tr. at 160:07-161:21 (May 27, 2015) (Hobbs; Charlesworth, USCO) (describing students adding three sentences of narrative over music videos); *id.* at 212:02-18 (Hobbs; Smith, USCO) (discussing use of footage of Roy Kroc).

[555] Future proponents may also wish to consider NTIA's query whether the proposed class needs to include all grades from K through 12, as opposed to starting at more upper level grades. *Id.* at 208:02-209:15 (Cheney, NTIA; Williams, Joint Creators; Hobbs).

For similar reasons, the record as presented does not establish the need for students or educators participating in media literacy or adult education programs outside of the school environment (Proposed Class 4) or students enrolled in MOOCs (Proposed Class 3) to circumvent access controls on DVDs, Blu-Rays, or digitally transmitted material.[556] While Hobbs pointed to the growing prevalence of media literacy studies, the few specific programs she cited did not appear to depend upon close analysis of motion picture excerpts; rather they seem to involve more general engagement with and manipulation of digital media, which can be accomplished through screen capture.[557] As for MOOCs, while proponents mentioned that in some cases enrollees may be tasked with video assignments, the Register finds that the record addressing proposed student (as opposed to instructor) uses is too indeterminate to support a recommendation for an exemption.[558]

Finally, while concluding on the current record that an exemption for screen-capture technologies should serve to facilitate the proffered uses by K-12 students and those teaching and participating in out-of-school educational programs, the Register notes that in appropriate contexts, such users may also be able to avail themselves of the noncommercial video exemption.[559]

The Register has previously determined that at least some types of screen-capture software are "comparable to camcording the screen—a process that has been identified as a noncircumventing option to accomplish noninfringing uses" because the images are captured after they have been decrypted.[560] But it is not clear that all screen-capture software operates in this fashion, and the record provides no absolute assurance that copyright owners would agree that specific types of software do not employ circumvention techniques.[561] More specifically, it appears that at least some screen-capture tools operate by circumvention, including when capturing content played on certain Apple devices, which incorporate proprietary content protection technologies.[562] Accordingly, the Register again finds that there is a need for exemptions to address the

[556] *Id.* at 234:11-25 (Hobbs); *see also* Hobbs Class 4 Reply at 5.

[557] Hobbs Class 4 Reply at 2-3, 8.

[558] *See* Joint Educators Class 3 Supp. at 8.

[559] *See* Tr. at 174:04-175:12 (May 27, 2015) (Hobbs; Charlesworth, USCO).

[560] 2010 Recommendation at 60-61; *see also* 2012 Recommendation at 134.

[561] Tr. at 70:19-71:13 (May 20, 2015) (Williams, Joint Creators; Charlesworth, USCO; Smith, USCO).

[562] *See, e.g.*, Joint Educators Class 1 Supp. at 16 ("TPMs block screen capture tools . . . ."); Tr. at 243:11-19 (May 28, 2015) (Tushnet, OTW) (stating WM Capture is "the only software that claims not to be circumvention"); Joint Educators Class 7 Post-Hearing Resp.; Joint Educators Class 3 Reply at 16; Tr. at 74:07-75:21 (May 28, 2015) (Benmark, Authors Alliance/Buster; Charlesworth, USCO) (discussing Apple technology); Tr. at 25:14-17 (May 27, 2015) (Band, LCA); Tr. at 76:03-77:14 (May 27, 2015) (Decherney, Joint Educators; Band, LCA; Taylor, DVD CCA; Charlesworth, USCO; Smith, USCO; Ruwe, USCO); Tr. at 59:01-15 (May 27, 2015) (Taylor, DVD CCA; Charlesworth, USCO); *but see* Tr. at 49:19-50:01 (May 27, 2015) (Taylor, DVD CCA; Smith, USCO).

possible circumvention of protected motion pictures when using screen-capture technology for noninfringing purposes.[563]

In addition to screen-capture technology, Joint Creators contend that services that provide online access to materials lawfully purchased in physical formats, including digital rights libraries and disc-to-digital services, are additional viable alternatives to circumvention. As explained in the record, these types of cloud-based services allow consumers to obtain high-definition versions of copyrighted works that they may have purchased on DVD or Blu-ray, meaning that the screen quality is presumably comparable or improved as compared to the physical copy of the work. At the hearings, opponents indicated that these services offer convenient ways for users to cue up clips for later playback.[564] The evidence thus indicates that these services may, in some circumstances, serve as alternatives to circumvention of physical discs, although current content offerings appear far from comprehensive.[565] While the Register appreciates that these steadily growing services may be useful in some cases, the record therefore indicates that such services cannot yet serve as reliable alternatives to circumvention for many of the proposed uses.

ii. Viability of Alternatives to AACS-Protected Blu-ray Discs

Having concluded that proponents have demonstrated a lack of adequate alternatives to circumvention for many of the proposed uses, the Register must next evaluate whether prospective users are likely to suffer adverse effects without the ability to circumvent Blu-ray discs, or whether their needs would be satisfied by limiting the exemptions to circumvention of DVDs or digitally transmitted material. While prior rulemakings have considered Blu-ray technology in passing, this triennial rulemaking does so with the benefit of a larger volume of evidence to consider, and with an eye toward the emergence of still higher-resolution 4K and Ultra HD formats,[566] which are being incorporated into streaming platforms and forthcoming Ultra HD Blu-ray discs.[567] The Register appreciates that the requests to circumvent Blu-ray technology raise complex questions relating to proponents' represented needs for an exemption as well as opponents' concerns regarding the potential effects of such an exemption; while

[563] *See* 2012 Recommendation at 134-135.

[564] Tr. at 163:09-25 (May 19, 2015) (Smith, USCO; Voris, The Walt Disney Studios; Charlesworth, USCO).

[565] Tr. at 47:04-48:12 (May 27, 2015) (Turnbull, AACS LA; Smith, USCO); Tr. at 124:03-126:04 (May 19, 2015) (Teitell, DECE and UltraViolet; Damle, USCO) (discussing market share of UltraViolet for new releases).

[566] 4K resolution generally refers to cinematic display devices (*i.e.*, movie projectors) that have a resolution of 4096 x 2160 pixels and approximately a 1.9:1 aspect ratio. UHD television is a separate standard with a close but not identical resolution of 3840 x 2160 and a 16:9 aspect ratio.

[567] In contrast to 4K and Ultra HD standards, high definition has a resolution of 1920 x 1080 pixels, and DVD has a resolution of 720 x 480 pixels. So, DVDs contain 345,600 pixels per video frame compared to 2,073,600 for Blu-ray or 8,294,400 for 4K and Ultra HD. Joint Filmmakers Supp. at App. B. Ultra HD Blu-ray is expected to be introduced within the next year.

opponents' concerns are discussed below in the context of the statutory factors, this section focuses on whether proponents have made their case.

Proponents generally seek to circumvent AACS-protected Blu-ray discs because Blu-ray content is of a higher quality than available alternatives (including circumvention of DVDs or digitally transmitted material) and/or because certain material may be available only on Blu-ray. The Register first evaluates whether proponents for derivative uses of motion picture excerpts—in filmmaking (Class 6), noncommercial videos (Class 7), and e-books (Class 5)—have demonstrated that they are likely to suffer adverse effects if denied an exemption to circumvent AACS-protected Blu-ray discs. Proponents of these derivative uses argue that accessing content on Blu-ray is necessary to create and/or distribute their own new and creative derivative works.

Joint filmmakers presented a detailed record to argue that standard-definition resolution is insufficient for film distribution purposes. The record contains references to HD (*i.e.*, Blu-ray) quality requirements from distributors such as CNN, BBC, NBC, Discovery Health, PBS, and various other entities, as well as examples where films or clips within programs were rejected because they were only standard-definition (*i.e.*, DVD) quality.[568] For example, Joint Filmmakers submitted a frame-by-frame analysis report from CNN analyzing a documentary film entitled *Life Itself* that rejected many embedded SD clips.[569] Joint Filmmakers also provide PBS' Technical Operating Specifications, which require HD or better resolution, and the record contains testimony from multiple filmmakers that PBS rejects footage submitted in SD.[570] Citing as an example a documentary on Roger Ebert, Joint Filmmakers also claim that distributors "often" reject material that has been "upconverted" from SD to HD.[571] Joint Filmmakers also explain that DVD quality is likely to become increasingly less acceptable as 4K resolution becomes widespread.[572] Based on this record, the Register finds that Joint Filmmakers have demonstrated they are likely to suffer adverse effects if they are unable to make use of material on Blu-ray in these cases.

Similarly, EFF/OTW contend that remix artists cannot achieve their proposed uses without access to Blu-ray, both because of image quality and content availability

---

[568] Tr. at 98:04-100:09 (May 20, 2015) (Morrissette, Kartemquin Educational Films) (providing example of BBC quality control process); *see also id.* at 9:21-23 (Morrissette, Kartemquin Educational Films) ("DVD quality images are being rejected on our programs by our distributors ranging from Magnolia Films to CNN."); *id.* at 51:02-53:10 (Neill, NMR; Charlesworth, USCO) (discussing international distributors and PBS); Joint Filmmakers Supp. at 16, App. I (providing statements from various filmmakers); Joint Filmmakers Reply at 8, Apps. C-D.

[569] Joint Filmmakers Reply at 8, App. D.

[570] *See id.* at 7-8 (citing PBS' specifications and explaining that "[e]xceptions are granted rarely and primarily in the context of archival footage that was not created in high definition"); Joint Filmmakers Supp. at App. I (testimony 4, 5, 14 from filmmakers re PBS).

[571] Tr. at 98:04-100:09 (May 20, 2015) (Charlesworth, USCO; Morrissette, Kartemquin Educational Films; Damle, USCO).

[572] *Id.* at 11:01-23 (Morrissette, Kartemquin Educational Films; Charlesworth, USCO).

concerns. Extensive interviews by remix artists were submitted, explaining that DVD-quality source material results in lost frames, grainy colors, pixilation and other artifacts that hinder or even preclude the application of complex editing effects.[573] For example, vidder JetPack Monkey explained that Blu-ray video was the only available source to obtain a version of the film *Halloween H20* that is in a similar format and aspect ratio to the other *Halloween* films, required for a vid that intercut scenes from films shot over a 40-year period.[574] EFF/OTW also explain that vidders often rely upon extra or bonus material available only on Blu-ray discs to create their narrative; for example, they reference a vidder who combined clips from the feature film and the Blu-ray bonus materials to form a message about the film *Captain America.*[575] As a general matter, EFF/OTW assert that users are entitled to "what is needed to accomplish their [non-infringing] purpose."[576] While AACS LA points out that fair use does not entitle users to the "optimum method" of copying,[577] there is a difference between "optimum" and "necessary," and the Register concludes that proponents have submitted an adequate factual record to demonstrate that, in certain cases, Blu-ray is required for remix artists to achieve their intended uses.

Considering proposed uses in e-books, the record demonstrates that e-book readers, such as the Kindle Fire, Kindle Voyage, Kobo Glo HD, or Apple iPad, offer resolution that is HD quality or higher and that a variety of e-books are currently marketed based on their HD content.[578] Proponents also demonstrate that Blu-ray content may be necessary for certain proposed film analysis uses in e-books, such as to analyze nuances in cinematography or sound editing, or to comment upon material available only on Blu-ray discs.[579] Although the record is less developed than for filmmaking or noncommercial videos, Class 5 proponents have demonstrated that, in some cases, accessing Blu-ray content may be required for the proposed uses of e-books containing film analysis.

---

[573] EFF/OTW Reply at 8-10, Apps. A-B. To the extent that EFF/OTW argue more broadly that aesthetic choice necessitates access to Blu-ray materials, the Register finds that the record presented was limited to more specific needs, such as the ability to portray fine-grained details, format films into the desired aspect ratio, or apply effects such as cropping, zooming, dissolves, or superimposition.

[574] *Id.* at 5.

[575] EFF/OTW Supp. at 25. EFF/OTW also submitted a list of materials available only through Blu-ray, compared to DVD.

[576] EFF/OTW Reply at 11 (citing *Campbell*, 510 U.S. at 588; *Bill Graham*, 448 F.3d at 613; *Warren Pub. v. Spurlock*, 645 F. Supp. 2d at 420, 425).

[577] *See* DVD CCA Class 7 Opp'n at 8 (citing *Corley*, 273 F.3d 429).

[578] Authors Alliance Reply at 6-7; Lerner/Reid Class 5 Post-Hearing Resp.

[579] *See, e.g.*, Authors Alliance Supp. at App. B (discussing cinematography in films such as *The Godfather*), App. C (re sound editing), App. E (listing Blu-ray only content, including added material in *James Bond* films, a proposed use of this class). By contrast, after comparing the DVD and Blu-ray examples of *The Shawshank Redemption* and *The King's Speech* offered by proponent Buster at the hearing, the Register finds the differences negligible at most and declines to credit these examples. *See* Tr. at 13:14-14:24, 16:01-17-21, Exhibit 22 (May 28, 2015) (Buster).

A separate question is whether the educational users, who may find screen-captured images unsuitable for some proposed uses, actually require Blu-ray images in order to perform their close analysis of the underlying work itself, or if standard-definition resolution is sufficient. In Classes 1 (colleges and universities) and 3 (MOOCs), Joint Educators submitted many instances where high-definition quality—as opposed to DVD quality—was necessary to closely analyze films including *The Wizard of Oz* (to highlight prop wires and other "stage-like" elements),[580] *Citizen Kane* (to appreciate depth of field, chiaroscuro effects, and subtle narrative elements),[581] Jacques Tati's *Playtime* (to better approximate the intended 70mm viewing experience and appreciate the film's very detailed and complex composition),[582] and *Saving Private Ryan* (to experience the enhanced color and contrast effect of bleach bypass film processing, hyper-realism, and complex soundscapes).[583] These examples seemingly apply to cinema studies in traditional physical classrooms as well as lectures in online learning contexts, as Joint Educators explain that students and faculty engage in "fundamentally the same kinds of activities, whether they are in a MOOC or in a traditional college or university classroom."[584] Based on this record, the Register determines that faculty and students participating in college or university classes, or faculty presenting MOOCs[585] are likely to suffer an adverse effect if unable to incorporate Blu-ray quality images when necessary for close analysis of film or media images.

As for the other proposed educational uses, Classes 2 (K-12) and 4 (museums, libraries and nonprofits) proponents submitted no examples where Blu-ray quality or Blu-ray-unique content was required for uses in K-12 classrooms or media literacy programs. For Class 2, the record contains only a single example where a high school teacher wished to compile clips of Shakespearean works taken from Blu-ray discs, but whose needs were able to be met by using DVDs.[586] For Class 4, the only reference to material available on Blu-ray concerns the television series *Orange is the New Black*, which is produced by and available on Netflix and thus is able to be alternatively accessed.[587] Accordingly, the Register concludes that the record does not establish there is a likely adverse impact for Proposed Classes 2 and 4 if the prohibition on circumventing AACS-protected Blu-ray discs remains.

---

[580] Joint Educators Reply at 10.

[581] *Id.* at 11.

[582] *Id.* at 12.

[583] Tr. at 26:23-27:13 (May 27, 2015) (Band, LCA); *id.* at 29:20-30:05 (Decherney, Joint Educators); *see* Joint Educators Class 1 Reply at 15.

[584] Joint Educators Class 3 Reply at 10.

[585] As explained above, the Register finds that the record does not sufficiently establish the need for participants enrolled in MOOCs to engage in circumvention of motion pictures.

[586] *See* Hobbs Class 2 Supp. at 4; Tr. at 183:13-20 (May 27, 2015) (Smith, USCO; Hobbs) (confirming that proponents did not offer any additional examples of proposed uses of Blu-ray discs).

[587] *See* Hobbs Class 4 Reply at 8.

c. Statutory Factors

The Register now turns to the statutory factors, which are reviewed collectively in relation to the several classes.

With respect to the first factor, the impact on the availability of copyrighted works, the Register previously "determined that it is questionable whether CSS protection is a critical factor in the decision to release motion pictures in digital format," noting that "DVDs remain the dominant form of distribution" despite the wide availability of circumvention tools.[588] Consistent with this finding, the current record suggests that the prior exemptions have not harmed the market for DVDs and, in fact, no party opposes renewing the current exemptions for DVDs. Accordingly, the Register finds that the record does not demonstrate that an exemption to circumvent CSS-protected DVDs will decrease the availability of copyrighted works.

Regarding the various systems protecting motion pictures available via online distribution services, the record demonstrates that these systems effectively control access to copyrighted works; however, the record also shows that decryption tools are widely available. As with DVDs, there is no evidence that the existing exemption authorizing circumvention of TPMs used by online distribution services has harmed the market or decreased new releases of copyrighted motion pictures.

With respect to Blu-ray discs, opponents assert that allowing an exemption is likely to undermine Blue-ray-related content because it will erode copyright owners' confidence in the AACS protection system and the Blu-ray disc format generally.[589] AACS LA argues that allowing circumvention of Blu-ray discs to create perfect copies of the entire work could harm the Blu-ray business model at a time when Blu-ray is still establishing its place in the overall motion picture market.[590] The Register agrees that access controls such as AACS play a significant role in copyright owners' ability to invest in and disseminate valuable copyrighted works. As discussed below, however, while this may be true as a general matter, the record does not reflect that allowing the uses proposed here will have a material impact on the efficacy of AACS technology or the ability to bring new Blu-ray content to market. Although the record indicates that AACS circumvention tools are not as accessible as CSS circumvention software and circumvention of Blu-ray is not as prevalent as circumvention of DVDs, [591]

[588] 2012 Recommendation at 135-36; *see also* 2010 Recommendation at 57 (stating that "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").

[589] *See, e.g.*, AACS LA Class 7 Opp'n at 18.

[590] *See, e.g.*, DVD CCA/AACS LA Class 3 Opp'n at 14-16 (asserting that circumvention could undermine "the continued growth of the market for Blu-Ray discs"); AACS LA Class 6 Opp'n at 22; AACS LA Class 7 Opp'n at 16-19.

[591] *See, e.g.*, Tr. at 77:21-78:25 (May 28, 2015) (Turnbull, AACS LA).

circumvention of the Blu-ray format is nonetheless possible and not uncommon, including among video artists.[592] The Register therefore cannot conclude on this record that allowing a limited exemption to make brief, transformative uses of motion pictures for noninfringing purposes would have a material impact on the availability of motion pictures on Blu-ray or of motion pictures generally.

Moreover, some of the proposed uses, including for filmmaking or noncommercial videos, will facilitate the creation of new copyrighted works. The record indicates that the overall availability of copyrighted works will not be lessened—and may in fact increase—if circumvention is permitted for certain limited purposes. Accordingly, the first statutory factor tends to favor appropriately tailored exemptions to permit the fair use of protected motion picture material.

Turning to the second statutory factor, the availability for use for nonprofit archival, preservation, and educational uses, this factor clearly favors the proposals relating to educational uses, as well as to a lesser degree those relating to documentary films and multimedia e-books offering film criticism, and perhaps some noncommercial videos. Overall, this factor also appears favorable vis-à-vis most of the proposed exemptions.

The third factor, the impact the prohibition on circumvention has on criticism, comment, news reporting, teaching, scholarship, and research, is a critical consideration in relation to noncommercial videos, filmmaking, multimedia e-books offering film criticism, and educational uses. Each of these categories seeks to enable the listed statutory purposes. This factor therefore weighs strongly in favor of properly crafted exemptions to foster such uses.

The fourth factor, the effect of circumvention on the market for or value of copyrighted works, is an important consideration with respect to each of the proposed uses. Motion pictures involve significant effort and expense to create and, as the proposals demonstrate, are a vital American art form. The motion picture industry has a legitimate interest in preventing works from being copied and used in ways that undermine the market for or value of these works, including the market for derivative uses. Significantly, however, in each class, the record reflects the need to use only brief portions of the protected works. Many examples in the record demonstrate uses of less than thirty seconds of footage,[593] representing a very modest amount of an entire film or

[592] *See, e.g.*, Tr. at 111:21-112:06 (May 20, 2015) (Swart, Twentieth Century Fox Home Entertainment; Ruwe, USCO); EFF/OTW Supp. at 2 ("Numerous tools exist to circumvent such restrictions."); Tr. at 195:01-03 (May 27, 2015) (McSherry, EFF) ("[A]rtists are already relying on Blu-ray source.").

[593] *See, e.g.*, EFF/OTW Supp. at App. A at 5 (citing soda_jerk remix video art); *id.* at 9 (re *Take it Away* video); Authors Alliance Supp. at App. B (Statement of Bobette Buster) (describing planned usage of fleeting clips of motion pictures in e-book series on filmmaking); Joint Educators Class 1 Supp. at 18 (describing use of a clip showing brief dissolve of one image into another from *The Soviet Story*); *see also*Joint Educators Class 1 Supp. at 12 (quoting Patricia Aufderheide, Professor of Communication Studies

television episode. As in the past, the Register concludes that the use of such small portions in contexts involving comment or criticism is consistent with principles of fair use and unlikely to supplant the market for motion pictures. At the same time, exemptions in this area must be carefully focused on noninfringing uses so as not to undermine copyright owners' ability to license portions of motion pictures for entertainment purposes and other derivative uses outside of the parameters of fair use, including through clip licensing services.

As noted above, opponents point to the integrity of access controls as an important factor in preserving the value of copyrighted works.[594] Speaking to market impact, opponents additionally observe that about "75-80 percent of Blu-ray revenue stems from the first two to four weeks of a title's distribution."[595] For their part, proponents analogize AACS-protected works to previous exemptions for CSS-protected DVDs to argue that an exemption is unlikely to harm the market for Blu-ray discs or affect the integrity of access controls.[596] It is worth noting that the proposed uses of excerpts across the various proposed classes do not appear to be particularly tied to "new releases," and indeed, often relate to classic or already popular films or television episodes. While the Register is sympathetic to opponents' concerns about the integrity of Blu-ray, the record does not establish a clear relationship between the circumvention of Blu-ray discs for limited noninfringing purposes such as those being proposed here and piracy of, or otherwise diminished markets for, copyrighted motion pictures. The Register therefore finds that the fourth factor does not strongly favor, but also does not weigh against, properly conceived exemptions to enable the use of motion picture excerpts for criticism and commentary.

The Register thus concludes that the statutory factors on the whole tend to favor appropriately tailored exemptions to foster noninfringing uses of motion picture excerpts.

4. NTIA Comments

NTIA recommends renewing the current exemptions for educational and derivative uses, and expanding those exemptions in several respects. As a general matter, NTIA proposes that the exemptions should encompass "motion pictures and similar audiovisual works" on DVDs, Blu-ray discs, and obtained via online distribution services. NTIA explains that expanding the exemptions to include Blu-ray is appropriate

---

in the School of Communication at American University, explaining that use of short clips was necessary to use classroom time efficiently).

[594] *See* DVD CCA/AACS LA Class 3 Opp'n at 14; Tr. at 128:02-16 (May 27, 2015) (Turnbull, DVD CCA/AACS LA); DVD CCA/AACS LA Class 4 Opp'n at 13-14; Joint Creators Class 4 Opp'n at 6; AACS LA Class 5 Opp'n at 14-15; DVD CCA Class 5 Opp'n at 12-13; Joint Creators Class 5 Opp'n at 6; AACS LA Class 6 Opp'n at 22-23; DVD CCA Class 6 Opp'n at 19-20; Joint Creators Class 6 Opp'n at 6.

[595] Tr. at 112:02-06 (May 20, 2015) (Swart, Twentieth Century Fox Home Entertainment) (stating the first two to four weeks "is where the vast majority of the Blu-ray business happens and then it drops off dramatically"); *see also* Tr. at 46:06-11 (May 27, 2015) (Turnbull, AACS LA; Smith, USCO).

[596] *See, e.g.*, Authors Alliance Reply at 8.

for the educational uses in Classes 1 to 4 because "the exclusion of high definition material is having an adverse effect on the quality of teaching."[597] NTIA claims that an expansion to Blu-ray is also appropriate for the derivative uses in Classes 5 to 7 because "the quality of clips obtained from DVDs is substantially less than that of Blu-ray," and because "film and television distribution standards . . . require use of high definition video."[598] For all classes, NTIA finds the alternatives to Blu-ray circumvention to be inadequate.[599]

At the same time, NTIA rejects proposals to expand the exemptions to encompass all "noninfringing" or "fair uses," instead favoring maintenance of "a tailored exemption."[600] It suggests "provid[ing] further clarity" in the exemption language, and proposes that the exemption be limited to circumvention conducted "solely to incorporate excerpts of such works into new works for the purpose of criticism, comment, or education, where the length of the clip is no more than reasonably necessary for such purpose and does not constitute a substantial portion of the original work."[601] In addition, by limiting its proposals to "motion pictures and similar audiovisual works," NTIA appears implicitly to reject proposals to expand the exemption to encompass all "audiovisual works," including video games.[602]

With respect to the specific classes, NTIA makes the following proposals, and in each case, NTIA recommends that the exemption permit circumvention of TPMs on DVDs, Blu-ray discs, and online distribution services. With respect to Class 1, NTIA proposes an exemption for "[e]ducational use by college and university instructors, faculty, and students."[603] Although the current exemption for colleges and universities distinguishes between uses in film studies and other courses requiring close analysis of film and media excerpts, and uses in other courses,[604] NTIA's proposed exemption does not.[605] NTIA does not explain, however, why elimination of that distinction is warranted.

For Class 2, NTIA proposes an exemption for "[e]ducational use by K-12 instructors, and by students in grades 6-12 engaging in video editing projects actively overseen by an instructor."[606] NTIA acknowledges that "[s]creen capture technology, despite its limitations, may be sufficient" for students "in certain circumstances."[607] It

[597] NTIA Letter at 14-15.

[598] *Id.* at 24.

[599] *Id.* at 14-17, 24-26.

[600] *Id.* at 13 & n.42.

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

[602] *Id.* at 14.

[603] *Id.*

[604] 37 C.F.R. § 201.40(b)(4)-(7).

[605] NTIA Letter at 14.

[606] *Id.*

[607] *Id.* at 17.

nonetheless asserts that circumvention should be permitted "when the project requires a level of quality only available through circumvention."[608] As discussed below, however, the Register concludes that the record lacks any specific evidence showing a need for such students to access anything more than screen-captured video clips.[609]

For Class 3, NTIA proposes an exemption for "[e]ducational use by instructors offering [MOOCs] engaged in film and media analysis."[610] NTIA notes that "online learning should be encouraged, as it allows a breakdown of the traditional barriers to education such as geographic restrictions and limited financial resources."[611] At the same time, it "recognizes the importance of crafting an exemption that is based on the record and will not be misinterpreted as covering every application and service on the Internet."[612] In particular, NTIA notes that "because any Internet user can enroll in a MOOC," there is "some concern that a poorly-crafted exemption could further infringement."[613] NTIA also concludes that "the record is too limited with respect to student needs to circumvent TPMs to complete class work while enrolled in MOOCS to support their inclusion at this time."[614] NTIA further "supports limiting the exemption to MOOCs that focus on film or media analysis or studies, which would still cover the desired uses noted in proponents' comments." According to NTIA, "further expansion of this exemption to all MOOCS is not supported on the record."[615]

NTIA also addresses the TEACH Act in relation to Class 3, concluding that incorporating that provision's limitations in a MOOC exemption would be inappropriate. First, NTIA observes that the provision "only applies to online course activities that are part of a governmental body or 'accredited nonprofit educational institution.'"[616] According to NTIA, "not all MOOCs will qualify" under that requirement.[617] To support that point, however, NTIA points only to extra-record evidence that National Geographic Society and the Museum of Modern Art provide courses through the Coursera platform;

---

[608] *Id.*

[609] Although NTIA suggests that student projects submitted for the National History Day competition are judged for "quality of the video," the published criteria it cites do not specifically reference video quality. *See id.* at 17 n.60 (citing *How an Entry Is Judged*, NATIONAL HISTORY DAY IN PENNSYLVANIA, http://pa.nhd.org/judging.htm (last visited Oct. 7, 2015)). Moreover, the specific criteria for documentaries only evaluates whether the submission is "original, clear, appropriate, organized and articulate" and whether "visual impact is appropriate to [the] topic." *See Documentary Evaluation Form*, NATIONAL HISTORY DAY IN PENNSYLVANIA, http://pa.nhd.org/images/uploads/Docu.pdf (last visited Oct. 7, 2015).

[610] NTIA Letter at 14.

[611] *Id.* at 18.

[612] *Id.*

[613] *Id.* at 19.

[614] *Id.*

[615] *Id.* at 19-20.

[616] *Id.* at 20.

[617] *Id.*

NTIA does not cite any evidence showing that these institutions need to engage in circumvention.[618] Second, NTIA argues that "the TEACH Act requirement to place TPMs on the embedded clips should not be included as a condition of an exemption," suggesting that "the record demonstrates that primary providers of MOOCs do not use TPMs for their online courses," and stating that given the other limitations that would be imposed under the exemption, it is "unconvinced that TPMs on MOOC content are necessary to prevent harm to the market for the original work excerpted in a lecture video."[619] As discussed below, contrary to NTIA, the Register finds based on the record that placing TPMs on such courses should not be unduly burdensome.

For Class 4, NTIA proposes an exemption for "[e]ducational use by instructors and students participating in digital media and literacy programs in libraries, museums, and non-profit organizations with an educational mission."[620] NTIA points to evidence regarding a poetry video project by YES PHILLY, a nonprofit GED program, in which students wish to incorporate clips of culturally relevant films.[621] In so doing, NTIA does not address why this evidence demonstrates the need for circumvention of TPMs on DVDs, Blu-rays, or online distribution platforms, rather than use of screen-capture technology. In any event, NTIA notes that the creation of such a video project "might be characterized as a noncommercial, remix video" under Class 7.[622]

For Classes 5 and 7, NTIA proposes renewing the existing exemptions for nonfiction or educational multimedia e-books offering film analysis, and for noncommercial videos, respectively, and expanding them to include Blu-ray discs.[623] NTIA does not specifically address the evidence presented in Class 5. With respect to the noncommercial video proposal in Class 7, NTIA notes that proponents "provided compelling material supporting their request," citing the "informative demonstration of the sophisticated video editing required to create their videos."[624]

Finally, for Class 6, NTIA proposes an exemption both for documentary films and for "[n]arrative films portraying real events, where the prior work is used for its biographical or historically significant nature."[625] NTIA acknowledges that it "is uncertain that the record supports including all narrative [films]."[626] Its proposed exemption is therefore limited to "biopics and other similar films" or in other fictional films where the use "is necessary to comment on the historically-based plot of the film, or

[618] *Id.*

[619] *Id.* at 21.

[620] *Id.* at 14.

[621] *Id.* at 22 & n.85.

[622] *Id.* at 22 n.85.

[623] *Id.* at 24.

[624] *Id.* at 26.

[625] *Id.* at 24.

[626] *Id.* at 27.

when necessary to show its biographical significance."[627] NTIA urges that "such uses are likely fair" under current case law, citing a case involving use of a film clip in a Broadway musical production.[628] NTIA does not, however, discuss the existing market for use of clips in films, or assess the effect the exemption would have on that market. Nor does it offer a definition of "biopic and other fictional films depicting historical events."[629] As discussed below, these concerns have led the Register to recommend against an exemption for non-documentary films.

Overall, the Register generally agrees with NTIA that the existing exemptions for uses of motion picture excerpts should be expanded in certain respects, though not as broadly as NTIA proposes, largely due to the limitations of the record.

5. Conclusion and Recommendation

As detailed above, proponents have sufficiently established that various technological measures interfere with their ability to make desired uses of motion pictures and that a significant number of those uses are likely fair and noninfringing. Proponents seeking exemptions for noncommercial videos, filmmaking, e-books offering film analysis, and certain educational uses have further established that they are, or are likely to be, adversely affected by the prohibition against circumvention, including when it is necessary to use high-quality motion picture material to convey intended criticism or commentary. In some, but not all cases, the intended use may require HD-quality content on AACS-protected Blu-ray discs.

Further, for those uses that do not require access to higher-quality content—a category that includes uses by educators and students who do not require close analysis of motion picture material—the Register finds that screen-capture technology has evolved to the point where it can fulfill these needs and, accordingly, recommends limited exemptions to address the possibility of circumvention when using such technology. The Register recognizes that it may be difficult to ascertain how particular technologies work. Indeed, the record does not include any examples of screen-capture technology that holds itself out as non-circumventing.

The specific recommendations are set forth below, and are influenced by the following considerations. Initially, to the extent proponents seek to exempt uses of motion pictures that exceed short portions of clips, the Register finds that these requests are not supported by the record, which is focused on brief excerpts. Moreover, the use of only short segments is critical to the Register's determination in this proceeding that a significant number of the desired uses are likely noninfringing.

---

[627] *Id.*

[628] *Id.* (citing *Sofa Entm't, Inc. v. Dodger Prods., Inc.*, 709 F.3d 1273, 1278 (9th Cir. 2013) (holding that use of an excerpt from *The Ed Sullivan Show* in a Broadway musical production of *Jersey Boys* was fair use)).

[629] *Id.*

Nor does the record support recommending an exemption for "audiovisual works" as opposed to the narrower category of "motion pictures," as these classes of works are defined in the Copyright Act. As explained above, proponents did not demonstrate a need to circumvent non-motion-picture audiovisual works in any of the classes. The Register finds that the category of motion pictures is sufficiently broad to cover the intended uses, in that it encompasses television programs and other forms of video in addition to feature-length films.

Similarly, to the extent proponents seek more expansive exemptions to cover generally "noninfringing" or "fair uses," these requests, too, lack support.[630] The evidence in each class focuses on transformative uses that provide criticism and commentary—that is, greater insights into—the underlying works. Consistent with the record presented in this rulemaking, then, the Register finds that the desire to engage in criticism or commentary is a critical factor in her recommendation to adopt the below exemptions. A mere requirement that a use be "noninfringing" or "fair" does not satisfy Congress's mandate to craft "narrow and focused" exemptions.[631] For this reason, the Register has previously rejected broad proposed categories such as "fair use works" or "educational fair use works" as inappropriate.[632] An exemption should provide reasonable guidance to the public in terms of what uses are permitted, while at the same time mitigating undue consequences for copyright owners.[633]

Turning to the multimedia e-books exemption specifically, the record contains no evidence of proposed uses in e-books that are not offering "film analysis," and the Register therefore sees no reason to deviate from the language of the previously granted exemption in this regard.

Next, in considering the noncommercial video exemption, although EFF/OTW suggest expanding the exemption to replace the term "noncommercial" with the phrase "primarily noncommercial," they fail to offer a rationale for such an expansion. Although they cite examples where commissions or exhibition stipends are paid to artists by noncommercial entities for noncommercial uses, it is not clear why these works would not be considered "noncommercial." Indeed, the current exemption states explicitly that "noncommercial videos include work created pursuant to a paid commission where a commissioning entity's use is noncommercial," and the Register believes this clarification should be continued.[634]

---

[630] *See, e.g.*, EFF/OTW Reply at 5-6.

[631] H.R. REP. NO. 105-551, pt. 2, at 38 (1998).

[632] 2006 Recommendation at 17-19.

[633] *See* Tr. at 13:12-15:25 (May 27, 2015) (Butler, Joint Educators; Charlesworth, USCO) (discussing role of regulatory language in providing user guidance); 2006 Recommendation at 19 (noting "if a class is too broad" it could "lead to undue harm to copyright owners" and would be "difficult to justify the exemption at all").

[634] 2012 Final Rule, 77 Fed. Reg. at 65,728; *see also* 2012 Recommendation at 141.

In addition, Joint Creators have suggested that the phrase "noncommercial videos" should be narrowed to help distinguish this category from the educational use exemptions.[635] Specifically, they propose revising the language of the exemption to limit it to uses of short portions of motion pictures "(i) in remix videos or mash-up videos involving parody or satire, (ii) in videos with overtly political messages, (iii) or in non-profit art museum installations or exhibitions."[636] Joint Creators believe that in 2012, the Register and the Librarian of Congress intended to limit this exemption to uses for "remix" purposes—that is, to videos that involve remixing or modifying a preexisting work or works in order to criticize or comment upon some aspect of the underlying work(s), or to make a broader societal or political statement.[637] Joint Creators concede, however, that they cannot say whether the current language has resulted in abuse of the exemption.[638] On this record, the Register concludes that Joint Creators' proposed amendment is unnecessary, and might unintentionally exclude otherwise permissible uses. The crux of the noncommercial exemption is that the use be a brief and transformative one for purposes of criticism or commentary; a remix video or a non-remix video may or may not fulfill these criteria. To the extent that a potential use might fall within both the noncommercial exemption and an educational exemption, it is unclear why that in itself should be of concern. In assessing whether circumvention is proper, the point is that the use fall under at least one exemption.

For the various educational exemptions, the Register finds it appropriate, based on the record presented, to continue to distinguish between purposes requiring close analysis of film and media excerpts and more general educational uses. As with prior rulemakings, the Register is limited to the record presented. The evidence demonstrates that screen-capture technology has markedly improved since the last proceeding and can serve as an adequate substitute to circumvention in cases where close visual or audio analysis of the excerpts is not required. In fact, screen capture may well be adequate to fulfill the majority of the educational uses at issue. As explained above, the Register finds that the evidentiary record for proposed uses in connection with K-12 students and media literacy after-school or adult education programs (apart from GED programs) is not well developed, and does not demonstrate that screen capture cannot meet these needs. Accordingly, the Register recommends a screen-capture exemption for these categories to address the possibility of circumvention when using this technology. In describing the users of motion pictures in such media literacy programs based on the record before her, the Register adopts proponents' refinement that the uses be connected to nonprofit digital and media literacy programs and adds the requirement that uses take place in the course of face-to-face instructional activities.[639]

---

[635] *See* Joint Creators Class 7 Post-Hearing Resp. at 2-3.

[636] *Id.* at 3.

[637] *Id.* at 2-3 (citing 2010 Recommendation at 37-38 and 2012 Recommendation at 106).

[638] Tr. at 300:10-301:14 (May 28, 2015) (Smith, USCO; Williams, Joint Creators).

[639] *See* Hobbs Class 4 Reply at 8; 17 U.S.C § 110(2).

For K-12 educators, the record was more robust in that proponents documented examples where high school educators relied upon DVD excerpts to facilitate classroom analysis of films such as *Citizen Kane* and *Chicago,* as well as other discussions of film theory, but proponents did not provide any examples where standard-definition resolution was insufficient to achieve these uses.[640] The Register therefore recommends an exemption to allow access by K-12 instructors to DVDs or digitally distributed material for purposes of close analysis. For college and university educators and students, and for education uses by faculty in connection with similarly situated MOOCs, the Register finds that the record demonstrates that access to Blu-ray discs may occasionally be required to engage in close analysis in cinema studies or similar courses if DVD or other standard-definition materials are insufficient to accomplish the desired analysis of visual or sonic details. But the record did not establish that students enrolled in MOOCs had a need to engage in circumvention to complete course assignments.

In evaluating the proposed exemption for MOOCs specifically, while the Register finds that the record establishes that MOOCs merit an exemption for the same reasons as college or university courses, the record does not support the sweeping approach suggested by proponents. Proponents' broadly framed proposal would seemingly encompass any online video that could be characterized as an educational experience. Upon examination of the record, however, the specific examples of proposed noninfringing uses submitted by the proponents all involve uses by faculty in courses offered by accredited educational bodies; although the Register is aware that some MOOCs operate independently of accredited organizations, no examples of purported noninfringing uses by these other (sometimes for-profit) MOOCs were provided to justify proponents' broad language. In addition, the Register is persuaded that while the strict contours of section 110(2) may be an imprecise fit for the rapid emergence of the MOOC model, section 110(2) nonetheless offers important and meaningful guidance concerning Congress's desire to balance pedagogical needs in distance learning with copyright owners' concerns of harmful impact. The Register therefore recommends that any exemption incorporate section 110(2)'s requirements that uses be limited to nonprofit educational institutions, that transmissions be limited to enrolled students, and that the transmitting body institute policies regarding copyright protection. Taking a further cue from the TEACH Act, the Register also recommends requiring MOOCs making use of this exemption to employ TPMs that reasonably prevent the retention and unauthorized dissemination of copyrighted content, as provided in section 110(2). In this regard, the Register notes that the record indicates that these measures should be relatively simple for course platforms to adopt.

Next, concerning uses by filmmakers, based on the extensive record presented, the Register recommends that the existing exemption for documentary films be continued. In considering non-documentary films, however, the Register concludes that the record does not support a finding that the use of motion picture clips in narrative films

[640] *See, e.g.*, Hobbs Class 2 Supp. at 5.

is, as a general matter, likely to be noninfringing. In light of documented concerns about the effect of such uses on existing markets, the Register cannot at this time recommend extending an exemption beyond non-documentary filmmaking. The Register observes, however, that the category of "documentary" should not be construed in an unduly narrow fashion,[641] and should be understood as sufficiently flexible to encompass films of this genre that incorporate limited scripted elements such as reenactments or imagined dialogue based on real events.

Further, for certain uses of motion picture excerpts obtained online, the Register recommends replacing the phrase "online distribution services" in the current exemption with the phrase "digitally transmitted video." This clarification is intended only to make clear that the exemption extends to online streaming video services, and is not intended to permit the making of full copies of works obtained from such services.

A number of commenters urged that the language of previous exemptions be simplified so that it is more accessible for users of the exemptions. The Register agrees, and has adopted the suggestion that exemptions be restructured based on the type of use at issue.[642]

Prospective users of the recommended exemptions should take pains to ensure that they satisfy each requirement of these narrowly tailored exemptions before seeking to invoke them. The Register encourages users to seek out and employ non-circumventing screen-capture technology or other technologies that can be employed in lieu of circumvention.[643]

Based on the foregoing analysis, the Register recommends that the Librarian designate the following classes:

> **Motion pictures (including television shows and videos), as defined in 17 U.S.C. 101, where circumvention is undertaken solely in order to make use of short portions of the motion pictures for the purpose of criticism or comment in the following instances:**
>
> **(i) For use in documentary filmmaking,**
>
> **(A) Where the circumvention is undertaken using screen-capture technology that appears to be offered to the public**

[641] *See generally* Class 6 Post-Hearing Responses (providing definitions of "documentary" films); *see also* ACADEMY OF MOTION PICTURE ARTS AND SCIENCES, 88TH ACADEMY AWARDS OF MERIT FOR ACHIEVEMENT DURING 2015, at 10 (2015), *available at* http://www.oscars.org/sites/default/files/88aa_rules.pdf (noting that a documentary film "may employ partial reenactment, stock footage, stills, animation, stop-motion or other techniques, as long as the emphasis is on fact and not on fiction").

[642] *See, e.g.*, Tr. at 297:14-19 (May 28, 2015) (Williams, Joint Creators).

[643] *See* 2012 Recommendation at 140 (same).

as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted, or

(B) Where the motion picture is lawfully made and acquired on a DVD protected by the Content Scramble System, on a Blu-ray disc protected by the Advanced Access Control System, or via a digital transmission protected by a technological measure, and where the person engaging in circumvention reasonably believes that screen-capture software or other non-circumventing alternatives are unable to produce the required level of high-quality content;

(ii) For use in noncommercial videos (including videos produced for a paid commission if the commissioning entity's use is noncommercial),

(A) Where the circumvention is undertaken using screen-capture technology that appears to be offered to the public as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted, or

(B) Where the motion picture is lawfully made and acquired on a DVD protected by the Content Scramble System, on a Blu-ray disc protected by the Advanced Access Control System, or via a digital transmission protected by a technological measure, and where the person engaging in circumvention reasonably believes that screen-capture software or other non-circumventing alternatives are unable to produce the required level of high-quality content;

(iii) For use in nonfiction multimedia e-books offering film analysis,

(A) Where the circumvention is undertaken using screen-capture technology that appears to be offered to the public as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted, or

(B) Where the motion picture is lawfully made and acquired on a DVD protected by the Content Scramble System, on a Blu-ray disc protected by the Advanced Access Control System, or via a digital transmission protected by a technological measure, and where the person engaging in circumvention reasonably believes that screen-capture software or other non-circumventing alternatives are unable to produce the required level of high-quality content;

(iv) By college and university faculty and students, for educational purposes,

(A) Where the circumvention is undertaken using screen-capture technology that appears to be offered to the public as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted, or

(B) In film studies or other courses requiring close analysis of film and media excerpts where the motion picture is lawfully made and acquired on a DVD protected by the Content Scramble System, on a Blu-ray disc protected by the Advanced Access Control System, or via a digital transmission protected by a technological measure, and where the person engaging in circumvention reasonably believes that screen-capture software or other non-circumventing alternatives are unable to produce the required level of high-quality content;

(v) By faculty of massive open online courses (MOOCs) offered by accredited nonprofit educational institutions to officially enrolled students through online platforms (which platforms themselves may be operated for profit), for educational purposes, where the MOOC provider through the online platform limits transmissions to the extent technologically feasible to such officially enrolled students, institutes copyright policies and provides copyright informational materials to faculty, students and relevant staff members, and applies technological measures that reasonably prevent unauthorized further dissemination of a work in accessible form to others or retention of the work for longer than the course session by recipients of a transmission through the platform, as contemplated by 17 U.S.C. 110(2),

(A) Where the circumvention is undertaken using screen-capture technology that appears to be offered to the public as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted, or

(B) In film studies or other courses requiring close analysis of film and media excerpts where the motion picture is lawfully made and acquired on a DVD protected by the Content Scramble System, on a Blu-ray disc protected by the Advanced Access Control System, or via a digital transmission protected by a technological measure, and where the person engaging in circumvention reasonably believes that screen-capture software or other non-circumventing alternatives are unable to produce the required level of high-quality content;

(vi) By kindergarten through twelfth-grade educators, including of accredited general educational development (GED) programs, for educational purposes,

(A) Where the circumvention is undertaken using screen-capture technology that appears to be offered to the public as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted, or

(B) In film studies or other courses requiring close analysis of film and media excerpts where the motion picture is lawfully made and acquired on a DVD protected by the Content Scramble System, or via a digital transmission protected by a technological measure, and where the person engaging in circumvention reasonably believes that screen-capture software or other non-circumventing alternatives are unable to produce the required level of high-quality content;

(vii) By kindergarten through twelfth-grade students, including those in accredited general educational development (GED) programs, for educational purposes, where the circumvention is undertaken using screen-capture technology that appears to be offered to the public as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted; and

(viii) By educators and participants in nonprofit digital and media literacy programs offered by libraries, museums and other nonprofit entities with an educational mission, in the course of face-to-face instructional activities for educational purposes, where the circumvention is undertaken using screen-capture technology that appears to be offered to the public as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted.

B. Proposed Classes 8 and 10: Audiovisual Works and Literary Works Distributed Electronically – Space-Shifting and Format-Shifting

1. Proposals

Proposed Classes 8 and 10 would allow circumvention of technological measures protecting motion pictures, e-books, and other audiovisual or literary works to allow users to view the materials on alternate devices for personal use or to create back-up copies.[644] Broadly speaking, this activity is referred to as "space-shifting" and, in some cases, "format-shifting." "Space-shifting" occurs when a work is transferred from one storage medium to another, such as from a DVD to a computer hard drive.[645] "Format-shifting" occurs when a work is converted into a new file or storage format, such as converting an e-book purchased through Amazon's Kindle store into a universally readable form.[646] Accordingly, the NPRM formulated these classes as seeking to engage in both space- and format-shifting.

Public Knowledge submitted a petition for an exemption to engage broadly in the noncommercial space-shifting of motion pictures.[647] Specifically, it seeks to allow consumers to transfer copies of motion pictures from DVDs, Blu-ray discs, or downloaded files to other digital formats so that the content can be viewed on alternate devices such as tablets, smartphones, and computers that lack DVD drives, or for backup purposes.[648] Another petition submitted by Alpheus Madsen requests an exemption to allow circumvention of access controls on DVDs specifically in order to play the DVDs on the Linux operating system.[649] Combining these two overlapping petitions, the NPRM described the class as follows:

---

[644] *See* Public Knowledge Space-Shifting Pet. at 2; Meadows Pet. at 1.

[645] One court has defined "space-shifting" as "mak[ing] copies in order to render [files] portable." *Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc.*, 180 F.3d 1072, 1079 (9th Cir. 1999); *see also* 2 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 8B.07[C][4] (rev. ed., 2015) ("2 NIMMER ON COPYRIGHT"). This is in contrast to "time-shifting," which the Supreme Court defined in the context of broadcast television as "record[ing] a program [one] cannot view as it is being televised and to watch it once at a later time." *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 421 (1984).

[646] *See, e.g.*, 2006 Recommendation at 80-83 (declining to recommend exemption for creation of back-up copies by both space- and format-shifting).

[647] Public Knowledge's proposed regulatory language reads as follows: "an exemption for digital rights management-encrypted motion pictures and other audiovisual works on lawfully made and lawfully acquired DVDs, Blu-ray discs ('BDs'), and downloaded files, when circumvention is accomplished for the purpose of noncommercial space shifting of the contained audiovisual content." Public Knowledge Space-Shifting Pet. at 1.

[648] *Id.* at 2; Madsen Pet. at 1; Public Knowledge Class 8 Supp. at 1-2.

[649] Madsen did not provide proposed regulatory language but stated "[a]s a user of the Linux Operating System, I cannot legally play DVDs I legitimately own, rent, or borrow, which is a violation of my free use of such DVDs." Madsen Pet. at 1. Madsen did not submit subsequent comments in this rulemaking.

> Proposed Class 8: This proposed class would allow circumvention of access controls on lawfully made and acquired audiovisual works for the purpose of noncommercial space-shifting or format-shifting. This exemption has been requested for audiovisual material made available on DVDs protected by CSS, Blu-ray discs protected by AACS, and TPM-protected online distribution services.[650]

Additional comments supporting this exemption were filed by the Music Library Association ("MLA"), Free Software Foundation ("FSF"), OmniQ, and over 130 individuals.[651]

Christopher Meadows submitted a petition for an exemption to engage in noncommercial space- or format-shifting of e-books.[652] This exemption would allow consumers to view e-books that are protected by TPMs on alternate viewing platforms and to create back-up copies. For example, it would allow a user to circumvent the TPM that restricts a book to a specific e-book reader in order to store a digital copy of it on a laptop or a different e-book reader. The NPRM described the exemption as follows:

> Proposed Class 10: This proposed class would allow circumvention of access controls on lawfully made and acquired literary works distributed electronically for the purpose of noncommercial space-shifting or format-shifting. This exemption has been requested for literary works distributed electronically [as] e-books.[653]

Comments supporting this exemption were filed by MLA, FSF, and Rachel Englander.[654]

Because the proposed space-shifting exemptions for audiovisual works and e-books involve common issues, Proposed Classes 8 and 10 are addressed together.

a. Background

The proposed classes here are similar to those sought in previous section 1201 rulemakings.[655] The Register has declined to recommend an exemption for such uses in

---

[650] NPRM, 79 Fed. Reg. at 73,862.

[651] MLA Class 8 Supp.; FSF Class 8 Supp.; OmniQ Reply; Arnold Scher Reply; David Butterworth Reply; David Graf Reply; Don Lowery Class 8 Reply; Gregory Borodiansky Class 8 Reply; James King Reply; Jason Weingartner Reply; John Berglund Reply; John Cleave Reply; Keith Chatfield Reply; Patrick Brett Class 8 Reply; Patrick Ferguson Class 8 Reply; Sandra Cobb Reply; Shawn White Reply; Valentin Duran Reply; Digital Right to Repair Class 8 Reply (118 individuals).

[652] Meadows specifically proposed that "[c]onsumers should be legally permitted to remove DRM from electronic books that they have purchased in order to back them up, read them on other e-book platforms, or otherwise make section 107 fair use of the material." Meadows Pet. at 1.

[653] NPRM, 79 Fed. Reg. at 73,863.

[654] MLA Class 10 Supp.; FSF Class 10 Supp.; Englander Supp.

[655] *See* 2012 Recommendation at 157; 2010 Recommendation at 214; 2006 Recommendation at 69; 2003 Recommendation at 126-27.

the past four rulemakings because the proponents have failed to establish a legal or factual record sufficient to establish that the space-shifting and/or format-shifting of audiovisual works, e-books, and other copyrighted works constitutes a noninfringing use.[656] When considering space- or format-shifting for the transfer of copyrighted works to different devices or the creation of back-up copies, the Register has consistently found insufficient legal authority to support the claim that these activities are likely to constitute fair uses under current law.[657]

In particular, the Register has previously noted that "no court has held that 'space-shifting' is a fair use,"[658] and that current law "does not guarantee access to copyrighted material in a user's preferred format."[659] In the 2012 rulemaking, the Register found that proponents had not adequately demonstrated that space-shifting was a transformative use as opposed to "simply a means for an individual consumer to access content for the same entertainment purpose as the original work."[660] While the Register has acknowledged that judicial interpretation of fair use could someday evolve to include certain space-shifting activities, as stated in the last proceeding, "the Section 1201 rulemaking process is not the forum in which to break new ground on the scope of fair use."[661]

The Register has also found in prior rulemakings that proponents failed to demonstrate any significant adverse effects resulting from the prohibition on circumvention,[662] failed to identify the specific DRM at issue,[663] or failed to show that the inability to access a copyrighted work was a result of an access control rather than software or hardware incompatibility.[664] At the same time, opponents in prior rulemakings have introduced evidence that market alternatives to circumvention—

---

[656] 2012 Recommendation at 162-65 (declining to recommend an exemption for space-shifting of audiovisual works on DVDs); 2010 Recommendation at 224 (declining to recommend an exemption for circumvention of access controls on DVDs and online streamed media to enable viewing on alternate platforms); 2006 Recommendation at 72, 80-83 (declining to recommend exemptions for space-shifting of audio and video content and for creation of back-up copies by both space- and format-shifting); 2003 Recommendation at 137, 141 (declining to recommend exemptions for space-shifting of "tethered" e-books, sound recordings, and audiovisual works).

[657] *See* 2006 Recommendation at 60, 69-72, 80-83; 2003 Recommendation at 130-31, 137-38.

[658] 2003 Recommendation at 130 (citing *Diamond Multimedia*, 180 F.3d at 1079); *see also* 2006 Recommendation at 70 (noting that the "commenters uniformly failed to cite legal precedent that establishes that such space-shifting is, in fact, a noninfringing use").

[659] 2012 Recommendation at 163 (citing *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 459 (2d Cir. 2001)); *see also* 2010 Recommendation at 224; 2006 Recommendation at 74; 2003 Recommendation at 132.

[660] 2012 Recommendation at 164.

[661] *Id.* at 163 (quotations omitted); *see also* 2003 Recommendation at 106.

[662] 2012 Recommendation at 165-66; 2010 Recommendation at 220, 223-24; 2006 Recommendation at 73-74; 2003 Recommendation at 134-138, 140-41.

[663] 2010 Recommendation at 220-21; 2006 Recommendation at 69.

[664] *Id.*

including peripheral devices, online downloading and streaming video services, set top boxes, cable and satellite on-demand services and, in the case of e-books, alternate formats, including hard copies of books—could mitigate the claimed adverse impact on accessibility.[665]

i. Proposed Class 8: Audiovisual Works

Public Knowledge's submissions are focused on enabling the viewing of feature films and television shows on tablets, smartphones, and laptops. Public Knowledge identifies several TPMs relevant to this class.[666] As with Classes 1 through 7, Class 8 proponents seek to circumvent CSS on DVDs and AACS on Blu-ray discs, both of which have been recognized as TPMs by the Register in previous proceedings.[667] Public Knowledge also identifies BD+ for Blu-ray discs, Content Protection for Recordable Media, and High-Bandwidth Digital Content Protection as additional TPMs that are applied to Blu-ray discs and digitally distributed content.[668] In addition to these specific TPMs, Public Knowledge requests the ability to circumvent "any DRM encryption standard" used to restrict copying of motion pictures.[669] With respect to downloaded files, Public Knowledge notes that a "wider variety of changing controls on digitally-delivered audiovisual works" is implicated and requests that the exemption not be overly specific, because foreclosing access to TPMs "that may be developed between now and 2018 would be unnecessarily limiting."[670]

Public Knowledge declined to specify the methods by which circumvention would be accomplished, arguing instead that the method of circumvention is irrelevant so long as the method would not "lead to infringing uses not within the intended scope of the proposal."[671]

---

[665] 2012 Recommendation at 165 (suggesting that "a reasonably priced peripheral, a different device, or an online subscription service to access and play desired content" may "offer a reasonable alternative to circumvention"); 2010 Recommendation at 221-23 & n.725 (discussing alternatives such as "online distribution and on-demand access," "streaming video," or "a set-top device"); 2006 Recommendation at 74 (discussing alternatives, including VHS format, "[o]nline access and online downloading," and "on-demand services from cable and satellite companies"); 2003 Recommendation at 132-33, 139-41 (discussing alternatives to e-book circumvention, including "hardcover, paperback, or audio book" and "multiple choices of formats, *e.g.*, Adobe Reader, Microsoft Reader, Palm Reader").

[666] *See* Public Knowledge Space-Shifting Pet. at 2; Public Knowledge Class 8 Supp. at 2.

[667] Public Knowledge Space-Shifting Pet. at 2; Public Knowledge Class 8 Supp. at 2; 2012 Recommendation at 126; 2000 Final Rule, 65 Fed. Reg. at 64,567-68.

[668] Public Knowledge Class 8 Supp. at 2.

[669] Public Knowledge Space-Shifting Pet. at 2.

[670] Public Knowledge Class 8 Supp. at 2.

[671] *Id.* at 3.

ii. Proposed Class 10: Literary Works Distributed Electronically

Meadows seeks to circumvent TPMs on e-books sold in the Kindle, Nook, and Kobo formats, which are allegedly locked by a "Digital Rights Management lock that encrypts the electronic books to prevent them from being read in unauthorized reader hardware."[672] However, neither he nor any other proponent provided further information as to the types of access controls used on e-books or the intended methods of circumvention.

b. Asserted Noninfringing Uses

i. Proposed Class 8: Audiovisual Works

Proponents claim that space- and format-shifting for personal, noncommercial uses, such as transferring audiovisual works from DVDs to alternate formats or creating back-up copies for preservation purposes, are established fair uses.[673] In support, Public Knowledge asserts that the "history of copyright legislation contains a multitude of references to noncommercial, personal uses," and argues that personal uses have long been considered noninfringing.[674] More specifically, Public Knowledge relies on a House Report[675] and hearing testimony of Register Barbara Ringer[676] regarding the 1971 Sound Recording Amendment to support the proposition that making noncommercial home audio recordings is a "recognized fair use."[677] From these sources, which address in relevant part whether the creation of a limited copyright in sound recordings could preclude home audio recording for private use, Public Knowledge infers support for a general space-shifting exemption in copyright law; in the view of Public Knowledge, the legislative history suggests that "it was clear that home users were . . . making personal copies from commercially-produced tapes and records," and "it would be nonsensical" to consider this copying onto alternate formats to be time-shifting as opposed to space- or format-shifting.[678] Public Knowledge also cites a 1961 Copyright Office Report, which

---

[672] Meadows Pet. at 2-3.

[673] *See* Public Knowledge Space-Shifting Pet. at 2; *see also, e.g.*, Cleave Reply at 1 ("I, personally, have had at least a dozen movies that I legally purchased become unusable due to defect or machine incompatibility: I ought to be allowed to make a backup to cover such an event."); Madsen Pet. at 4.

[674] Public Knowledge Class 8 Supp. at 3.

[675] *Id.* (quoting H.R. REP. NO. 92-487, at 7 (1971) ("1971 House Report") ("[I]t is not the intention of the Committee to restrain the home recording, from broadcasts or form tapes or records, of recorded performances, where the home recording is for private use and with no purpose of reproducing or otherwise capitalizing commercially on it.")).

[676] *Id.* at 4-5 (quoting *Prohibiting Piracy of Sound Recordings: Hearings on S. 646 and H.R. 6927 before the Subcomm. No.3 of the H. Comm. on the Judiciary*, 92d Cong. 22 (1971) (statement of Barbara Ringer, Assistant Register of Copyrights) ("1971 Testimony of Barbara Ringer") ("[Home video recording] is something you cannot control.")).

[677] *Id.* at 5.

[678] *Id.* at 4.

referenced the then-emerging ability to view private performances of televised motion pictures captured by home recordings, as further evidence of a space-shifting privilege.[679] Public Knowledge opines that "the most viable statutory rationale" for these various statements "has always been fair use."[680]

Public Knowledge further contends that case law establishes that space- and format-shifting are fair uses.[681] As in previous petitions, Public Knowledge relies upon *Recording Industry Association of America v. Diamond Multimedia Systems Inc.*[682] and *Sony v. Universal*,[683] although Public Knowledge concedes that the Register and the Librarian found that those cases "did not indicate that format-shifting and space-shifting were lawful, fair uses" in the 2012 rulemaking.[684]

Public Knowledge also points to a more recent district court decision in a case involving the satellite television provider Dish, *Fox Broadcasting Co. v. Dish Network LLC*,[685] as further support for its claim that the "noncommercial, nonprofit, private reproduction of the works onto a personal computing device" is a fair use.[686] The space-shifting service at issue in the *Dish* litigation was called "Hopper Transfers," and allowed Dish's subscribers to download content, including copyrighted television programming, from their Dish-provided set-top box onto personal devices such as a laptop, tablet, or smartphone.[687] Fox brought suit against Dish for copyright infringement and breach of contract; while the district court granted Dish's motion for partial summary judgment as to the copyright claim—indicating that the noncommercial "time- and place-shifting of recordings" at issue were fair use—it nonetheless found against Dish on the related contract claim.[688]

Notably, Public Knowledge's legal theory is not limited to the context of audiovisual works sold in digital formats. Instead, as made clear at the hearing, Public Knowledge believes that fair use would also entitle purchasers of physical books to make

---

[679] *Id.* (quoting U.S. COPYRIGHT OFFICE, 88TH CONG., REP. OF THE REGISTER OF COPYRIGHTS ON THE GENERAL REVISION OF THE U.S. COPYRIGHT LAW 30 (Comm. Print 1961) ("1961 Copyright Office Report") ("New technical devices will probably make it practical in the future to reproduce televised motion pictures in the home. We do not believe the private use of such a reproduction can or should be precluded by copyright.")).

[680] *Id.* at 5.

[681] *Id.* at 5-6; Public Knowledge Class 8 Reply at 2; OmniQ Reply at 5-9.

[682] *Diamond Multimedia*, 180 F.3d 1072.

[683] *Sony*, 464 U.S. 417.

[684] Public Knowledge Class 8 Supp. at 3.

[685] *Fox Broad. Co. v. Dish Network LLC*, No. CV 12-4529 DMG SHX, 2015 WL 1137593 (C.D. Cal. Jan. 20, 2015).

[686] Public Knowledge Class 8 Supp. at 6; *see also* Public Knowledge Class 8 Reply at 3-5.

[687] *See Dish*, 2015 WL 1137593, at *6.

[688] *Id.* at *30-31 (citing *Diamond Multimedia*, 180 F.3d at 1079).

full photocopies of them for purposes of convenience, although it could not provide specific case law authorizing such conduct.[689]

That said, Public Knowledge argues generally that the four-factor fair use test of section 107 validates its proposal.[690] Under the first factor, the purpose and character of the use, Public Knowledge urges that *Dish* and *Sony* indicate that space-shifting is a fair use because "the noncommercial, nonprofit, private nature" of a reproduction made for personal use "creates a presumption of fairness."[691] Public Knowledge did not address the second factor, the nature of the copyrighted work, or the third factor, the amount and substantiality of the use—although it is clear that Public Knowledge is seeking to create entire copies of expressive copyrighted works. As for the fourth factor, the effect on the market for or value of the work, Public Knowledge contends that "the harms for the market for copyrighted works remain speculative."[692] In support, Public Knowledge points to the *Dish* court's determination that Fox did not show more than a "speculative" market harm and also asserts that an exemption would "create a minuscule amount of market effect, due to the current prevalence of space-shifting" undertaken by consumers even without an exemption.[693]

Proponents of this exemption briefly present other arguments besides fair use to establish that their desired uses are noninfringing.[694] Commenter OmniQ submitted a patent application that purports to set forth a system of "non-reproductive" space-shifting, such that the original instance of a work is destroyed or made unusable when a copy of the work is moved to a new medium. OmniQ asserts that use of such a system would not implicate any of the exclusive rights under section 106 because "[t]here is no 'reproduction or duplication.'"[695] Although described in written comments, this system was not demonstrated at the hearings, and it is not clear from the record that a product embodying the patent specification has been made available for potential users or even prototyped.

---

[689] Tr. at 150:18-22 (May 19, 2015) (Siy, Public Knowledge).

[690] Public Knowledge Class 8 Supp. at 6.

[691] *Id.*

[692] *Id.*

[693] *Id.* at 6-7.

[694] *See id.* at 8-12 (arguing that agreement terms restricting consumers' personal use of purchased works are invalid and expressing concern that crediting these agreements in the rulemaking process would encourage copyright misuse); *see also* OmniQ Reply at 5 (arguing that the private performance of a work is "*always* noninfringing").

[695] OmniQ Reply at 1, 5-9 (citing *C. M. Paula Co. v. Logan*, 355 F. Supp. 189 (N.D. Tex. 1973) and *Lee v. Deck the Walls, Inc.*, 925 F. Supp. 576, 580 (N.D. Ill. 1996), *aff'd sub nom. Lee v. A.R.T. Co.*, 125 F.3d 580 (7th Cir. 1997)).

ii. Proposed Class 10: Literary Works Distributed Electronically

In his petition, proponent Meadows asserts that reading e-books on other devices and "archiving them in a universally-readable form against the possibility the current e-book vendor will go out of business" are forms of space- and format-shifting and, as such, are fair uses.[696] While Meadows briefly references the *Sony* and *Diamond Multimedia* decisions in his petition, he did not file supporting comments.[697] Other commenters submitted brief statements expressing their desire to create back-up copies of e-books for personal or library uses, but did not specifically address or explain how those uses were noninfringing.[698]

c. Asserted Adverse Effects

i. Proposed Class 8: Audiovisual Works

Public Knowledge argues that preventing users from engaging in fair use of purchased media is itself an adverse effect under section 1201.[699] Public Knowledge contends that "the monetary costs to consumers who avail themselves of . . . alternatives [are] real," as consumers will be forced to spend millions of dollars purchasing duplicate copies of audiovisual works and will lose billions of dollars in decreased utility (such as the ability to transfer files) without an exemption.[700] Public Knowledge explains that DVD drives are becoming less common on modern devices and suggests that consumers will be forced to buy "duplicate, expensive computing devices."[701] Public Knowledge conceded, however, that a consumer who wishes to "rip" a DVD would need some sort of DVD drive to do so.[702] In addition, Public Knowledge argues that because DVD and

---

[696] Meadows Pet. at 4.

[697] *Id.*

[698] Englander Supp. at 1 (noting that "[a] library should be able to take preventive measures to ensure the continued access of its information by its patrons"); MLA Class 10 Supp. at 1 (stating "[a]s e-book readers and file formats become obsolete, and as permissible under section 108, music librarians need to create preservation copies of textual works"); FSF Class 10 Supp. at 1 (stating that "[u]sers should be able to view or edit literary works in a free format").

[699] Public Knowledge Class 8 Supp. at 12.

[700] Tr. at 89:07-21 (May 19, 2015) (Siy, Public Knowledge); *see also* Public Knowledge Class 8 Supp. at 12-13; Public Knowledge Space-Shifting Pet. at 3; Duran Reply at 1 ("[I do not] have the means, that would allow me to re-purchase any of the DVDs in my collection."). Public Knowledge also argues that "when consumers buy a DVD or Blu-ray disc, they are buying a copy of a work which they own outright," in response to the assertion by the DVD Copy Control Association and the Advanced Access Content System Licensing Administrator ("DVD CCA/AACS LA"), who submitted a joint filing, that consumers are purchasing the right to access a copyrighted work. Public Knowledge Class 8 Reply at 6; *see also* DVD CCA/AACS LA Class 8 Opp'n at 4-5.

[701] Public Knowledge Class 8 Supp. at 13; *see also* Public Knowledge Space-Shifting Pet. at 3.

[702] Tr. at 156:22-157:18 (May 19, 2015) (Charlesworth, USCO; Siy, Public Knowledge); *see also* Public Knowledge Class 8 Supp. at 7-8 n.20 (citing *Copy A DVD*, WIRED, http://howto.wired.com/wiki/Copy_a_DVD (last visited Oct. 7, 2015) and Whitson Gordon, *How to Rip a DVD to Your Computer*, LIFEHACKER (Feb. 21, 2014), http://lifehacker.com/5809765/how-to-rip-a-dvd-to-your-computer).

Blu-ray discs degrade over time, in order to preserve their content, "consumers need to be able to extract those contents and shift them to a different format."[703]

Public Knowledge further claims that alternatives to circumvention, such as the streaming services, disc-to-digital services, and cloud-based digital rights locker services discussed below, are inadequate to remedy these harms.[704] Public Knowledge notes that many works are unavailable through streaming services, and that those that are may only be available intermittently or through the use of multiple pay services.[705] Additionally, Public Knowledge asserts that those titles that are offered by online services may not be practically available to all users due to lack of adequate broadband, ISP data caps, or incompatible hardware and software platforms.[706]

ii. Proposed Class 10: Literary Works Distributed Electronically

Proponents of Class 10 contend that consumers risk losing access to purchased e-books in the event that an e-book company fails and a backup copy cannot be made or the format becomes incompatible with future devices.[707] Proponents did not offer any specific examples of works that could not be accessed; however, Meadows further asserts that users are unfairly tied to one manufacturer's e-book device by the inability to render e-books purchased for use on one type of device, such as a Kindle, compatible with a new device, such as a Nook.[708]

d. Argument Under Statutory Factors

i. Proposed Class 8: Audiovisual Works

Proponents claim that the statutory factors set forth in section 1201(a)(1) support the granting of this exemption. First, proponents explain that the exemption will enhance the availability of copyrighted works because large quantities of works are only available in DVD format and are purportedly inaccessible to consumers whose devices lack DVD drives.[709] Second, regarding the availability for use of works for nonprofit archival, preservation, and educational purposes, proponents argue that "[a]llowing personal space-shifting creates a more robust environment for the preservation of works."[710] Third, with

[703] Public Knowledge Space-Shifting Pet. at 3-4.

[704] Public Knowledge Class 8 Supp. at 14-19.

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

[706] *Id.* at 15-19. Public Knowledge also notes there is no central data source that is comprehensive and up-to-date that lists where works are available. *See* Public Knowledge Class 8 Reply at 8, App. A.

[707] Englander Supp. at 1; Meadows Pet. at 5 (contending that a number of e-book stores have gone out of business in recent years).

[708] Meadows Pet. at 5.

[709] Public Knowledge Class 8 Supp. at 20; OmniQ Reply at 9.

[710] Public Knowledge Class 8 Supp. at 20; *see also* MLA Class 8 Supp. at 1; MLA Class 10 Supp. at 1; OmniQ Reply at 10-11.

respect to the impact of the prohibition on criticism, comment, news reporting, teaching, scholarship or research, Public Knowledge states that "while the primary purpose of the use in this exemption is purely personal, the proliferation of privately-held and compatible copies serves as a redundancy measure that helps protect potential later uses for these other fair uses."[711] Fourth, proponents argue that the value of the works for purchasers would increase as a result of an exemption, and that any predicted harm to copyright owners is merely speculative since consumers already engage in space-shifting even without an exemption.[712]

ii. Proposed Class 10: Literary Works Distributed Electronically

No Class 10 proponent directly addressed the statutory factors.

2. Opposition

a. Proposed Class 8: Audiovisual Works

Proposed Class 8 is opposed by DVD CCA/AACS LA and Joint Creators.[713] All of the Class 8 opponents take the position that this exemption should be rejected "in its entirety," noting that in the past the Librarian has repeatedly declined to grant this class.[714]

i. Asserted Noninfringing Uses

Opponents argue that space- and format-shifting are not established fair uses.[715] DVD CCA/AACS LA explain that consumers do not have an "unqualified right to access a work on a particular device," but instead purchase "only the right to access the work according to the format's particular specifications."[716] They argue that "[c]onsumers are able to purchase [a DVD or Blu-ray disc] at its retail price because it is distributed on a specific medium that will play back on only a licensed player," thus suggesting that retail prices would have been set higher if the seller intended to convey to purchasers the ability to view the copyrighted work in all potential formats.[717] DVD CCA/AACS LA dispute Public Knowledge's interpretation of legislative history, explaining that the 1971 Sound Recording Act concerns only "the creation of the sound recording right" and that

[711] Public Knowledge Class 8 Supp. at 20; *see also* OmniQ Reply at 11-12.

[712] Public Knowledge Class 8 Supp. at 6-8, 20-21; OmniQ Reply at 12; Tr. at 91:08-23 (May 19, 2015) (Siy, Public Knowledge).

[713] The trade groups represented by Joint Creators are the Motion Picture Association of America, the Entertainment Software Association, and the Recording Industry Association of America.

[714] Joint Creators Class 8 Opp'n at 2; DVD CCA/AACS LA Class 8 Opp'n at 2.

[715] DVD CCA/AACS LA Class 8 Opp'n at 4-8; Joint Creators Class 8 Opp'n at 3-4. Joint Creators, however, express a willingness to consider a future class proposal if it were tailored to archival preservation uses and tracked the language of section 108. Joint Creators Class 8 Opp'n at 3 n.3.

[716] DVD CCA/AACS LA Class 8 Opp'n at 4-5.

[717] *Id.* at 5; *see also* Tr. at 104:01-07 (May 19, 2015) (Turnbull, DVD CCA/AACS LA) (same).

the 1961 Copyright Office Report "does not constitute legislative history for any law that Congress ultimately approved."[718] Joint Creators stress that "not one of the four factors weighs in favor of a conclusion that space-shifting and format-shifting are fair uses."[719]

Opponents further assert that *Dish* does not alter the fair use status of space-shifting or format-shifting. They argue that the decision is erroneous because it equates space-shifting with time-shifting under *Sony* and mischaracterizes *Diamond Multimedia* as holding that space-shifting is a fair use under section 107 as opposed to a fair personal use under the Audio Home Recording Act of 1992 ("AHRA").[720] In addition, DVD CCA/AACS LA urge that, even if correct, the *Dish* opinion is distinguishable, because the Hopper Transfers service at issue imposed many restrictions on copying works to other devices and was limited to verified current subscribers, whereas the proposed exemption would make protected content "entirely freed, forever, from any restraints on consumer use."[721] DVD CCA/AACS LA also suggest that the fair use ruling in *Dish* was dicta: only a small portion of the *Dish* decision addressed space-shifting, and the court ultimately decided the case in the copyright holders' favor, "essentially holding that the contractual arrangement between the parties superseded the fair use finding, thus negating any practical effect of the fair use conclusions."[722] Opponents finally note that the *Dish* case is currently stayed pending settlement negotiations and is "far from concluded."[723]

ii. Asserted Adverse Effects

Opponents assert that proponents have failed to show that access controls have adverse effects on noninfringing uses, particularly in the face of available market alternatives.[724] Opponents provide examples of numerous alternatives to circumvention that provide digital audiovisual content, including (1) digital rights locker services such as UltraViolet and Disney Movies Anywhere, which allow consumers to verify their purchases of physical discs and subsequently download or stream verified films onto multiple devices;[725] (2) disc-to-digital services like VUDU or Flixter that allow

[718] DVD CCA/AACS LA Class 8 Opp'n at 5-6.

[719] Joint Creators Class 8 Opp'n at 3-4 (citing to previous 1201 rulemakings).

[720] DVD CCA/AACS LA Class 8 Opp'n at 6-8; Joint Creators Class 8 Opp'n at 4; *see also* Tr. at 138:18-139:11 (May 19, 2015) (Turnbull, DVD CCA/AACS LA).

[721] DVD CCA/AACS LA Class 8 Opp'n at 6-7; Tr. at 101:21-23 (May 19, 2015) (Williams, Joint Creators).

[722] DVD CCA/AACS LA Class 8 Opp'n at 7-8 n.4.

[723] *Id.* at 7; *see also* Joint Creators Class 8 Opp'n at 4; Tr. at 101:05-07 (May 19, 2015) (Williams, Joint Creators); Tr. at 139:15-20 (May 19, 2015) (Turnbull, DVD CCA/AACS LA). The Office notes that the stay in the *Dish* case automatically lifted on October 1, 2015, after the record in this rulemaking was closed. *See* Order Re Second Joint Status Report, No. CV 12-4529 DMG SHX (C.D. Cal. Sept. 30, 2015).

[724] DVD CCA/AACS LA Class 8 Opp'n at 8-10; Joint Creators Class 8 Opp'n at 4-5.

[725] DVD CCA/AACS LA Class 8 Opp'n at 8-10; Joint Creators Class 8 Opp'n at 5-9, Exhibits 1-6; Tr. at 105:06-16 (May 19, 2015) (Williams, Joint Creators); Tr. at 129:05-130:02 (May 19, 2015) (Voris, The Walt Disney Studios). Opponents claim that almost 20 million households in the United States use

consumers to convert their already purchased DVD or Blu-ray discs to high-quality digital files for a small fee, and then access those copies from a range of participating retailers;[726] (3) "download-to-own" video services such as Google Play, iTunes, and Amazon;[727] (4) online streaming services such as Hulu, Amazon Instant Video, or Netflix;[728] and (5) "TV Everywhere"-type services that allow subscribers to access movies and television programs on various platforms and devices on-demand or through live streaming.[729] Opponents suggest that as a general matter, these various services are rapidly growing, both in terms of number of users and catalog sizes, and comprise reasonable alternatives to circumvention.[730]

iii. Argument Under Statutory Factors

Opponents additionally argue that the statutory factors under section 1201(a)(1) militate against the proposed exemption. First, Joint Creators contend that "the use of access controls has facilitated wider availability of copyrighted motion pictures" as well as digital copying methods in the marketplace that do not involve circumvention.[731] Opponents do not directly address the second or third factors concerning the impact of the prohibition on preservation or criticism.[732] With respect to the fourth factor, DVD CCA/AACS LA argue that an exemption would harm the market for DVD and Blu-ray discs because circumvention results in "a perfect copy of the work being 'in the clear'" that can be "freely copied and redistributed" and would ultimately "reduce the number of copyrighted works distributed through market channels."[733]

Under the fifth factor, directing the Librarian to examine "such other factors as the Librarian considers appropriate,"[734] opponents argue that granting an exemption would undermine the purposes of section 1201 because "the DMCA was intended to encourage digital business models . . . that depend upon robust access control measures in order to increase consumer options and promote the flow of copyrighted materials to the

---

UltraViolet to access "over 130 million movies and TV shows" and that hundreds of films are available through Disney Movies Anywhere. Tr. at 121:19-24 (May 19, 2015) (Teitell, DECE/UltraViolet); *see also* Joint Creators Class 8 Opp'n at Exhibit 3.

[726] Joint Creators Class 8 Opp'n at 7, Exhibits 4-5; Tr. at 116:23-117:06 (May 19, 2015) (Teitell, DECE/UltraViolet); Tr. at 130:15-131:06 (May 19, 2015) (Voris, The Walt Disney Studios).

[727] DVD CCA/AACS LA Class 8 Opp'n at 9-10; Joint Creators Class 8 Opp'n at 8.

[728] DVD CCA/AACS LA Class 8 Opp'n at 10; Joint Creators Class 8 Opp'n at 8; *see also* Tr. at 110:22-111:09 (May 19, 2015) (Teitell, DECE/UltraViolet).

[729] DVD CCA/AACS LA Class 8 Opp'n at 10; Joint Creators Class 8 Opp'n at 7-8, Exhibit 6.

[730] *See, e.g.*, Joint Creators Class 8 Opp'n at 4-5.

[731] *Id.* at 7.

[732] *See* 17 U.S.C. § 1201(a)(1)(C)(ii)-(iii).

[733] DVD CCA/AACS LA Class 8 Opp'n at 11-12; *see also* Tr. at 141:03-17 (May 19, 2015) (Turnbull, DVD CCA/AACS LA).

[734] 17 U.S.C. § 1201(a)(1)(C)(v).

public."[735] DVD CCA/AACS LA assert that an exemption would "undermine" established licensing regimes for CSS and AACS by inhibiting these licensors from enforcing standard licensing terms, such as prohibitions on including DVD or Blu-ray copiers in products, or otherwise ensuring the uniformity of the licensing systems.[736]

b. Proposed Class 10: Literary Works Distributed Electronically

Proposed Class 10 was opposed by Joint Creators and the Software & Information Industry Association ("SIIA"). Opponents of this class maintain that proponents have failed to support their allegations of harm or their claims that space-shifting and format-shifting are noninfringing uses with sufficient factual or substantive legal arguments.[737] Opponents note that the Librarian has repeatedly concluded in previous rulemakings that "there is no basis under the law to conclude that back-up copying, format-shifting and space-shifting are fair uses,"[738] and argue that proponents have not presented any "new evidence, legal arguments or legal authorities in support of the exemption."[739]

3. Discussion

The Register recognizes the consumer and policy appeal of the proposed exemptions.[740] Consumers may feel frustrated when they purchase a movie or book in one format and are unable to watch that movie or read that book in a different format on another device. Recognizing this consumer interest, some countries have adopted private copying exceptions, which are often paired with schemes to compensate rightsholders through levies on blank media or copying equipment.[741] The United States itself in 1992 enacted AHRA to compensate copyright owners for the private copying of music on certain types of digital media.[742]

---

[735] Joint Creators Class 8 Opp'n at 9; *see also* DVD CCA/AACS LA Class 8 Opp'n at 12-13.

[736] DVD CCA/AACS LA Class 8 Opp'n at 13-16 (referencing court decisions enjoining Kaleidescape and Real Networks).

[737] Joint Creators Class 10 Opp'n at 2; SIIA Class 10 Opp'n at 1.

[738] Joint Creators Class 10 Opp'n at 2.

[739] SIIA Class 10 Opp'n at 1.

[740] The Copyright Office received over 150 comments in support of Class 8.

[741] *See* WORLD INTELL. PROP. ORG., INTERNATIONAL SURVEY ON PRIVATE COPYING (2013), *available at* http://www.wipo.int/edocs/pubdocs/en/copyright/1037/wipo_pub_1037_2013.pdf (surveying private copying exceptions and related compensation schemes in 32 countries). The EU InfoSoc Directive states that EU member states may exempt "certain types of reproduction of audio, visual and audiovisual material for private use, accompanied by fair compensation." *See* Directive 2001/29, of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, 2001 O.J. (L 167), 38 (EC). The UK enacted a private use exemption in 2014; however, the UK High Court recently held it to be unlawful because a compensation mechanism was not included. *British Academy of Songwriters, Composers and Authors v. Secretary of State for Business, Innovation and Skills*, [2015] EWHC 1723 (Admin), *available at* https://www.judiciary.gov.uk/wp-content/uploads/2015/06/basca-v-sofs-bis-judgment.pdf.

[742] *See* AHRA, Pub. L. No. 102-563, 106 Stat. 4237 (1992) (codified at 17 U.S.C. §§ 1001-1010).

At the same time, the section 1201 rulemaking is a carefully tailored proceeding that is designed to incorporate, not replace, the determinations of Congress and the courts. In reviewing the law, the Register does not find any fair use precedent that sanctions broad space-shifting or format-shifting. Moreover, as part of that proceeding, the Register must recognize marketplace efforts to meet consumer demand by providing alternative solutions, including a wide range of services that offer digital distribution of movies, television shows, and books under varying pricing schemes that motivate copyright owners to invest in future markets.[743] There are also services that convert DVD and Blu-ray discs to online formats.[744] Many of these offerings are significantly more evolved than at the time of the last rulemaking.[745]

These marketplace developments confirm that the policy judgments surrounding the creation of a novel exception for space- or format-shifting of copyrighted works are extremely complex and not at all self-evident.[746] Further, as explained more fully below, proponents have failed to meet their burden to show adverse effects that are the result of TPMs.

a. Noninfringing Uses

The legislative history relied upon by Public Knowledge does not support its claim that space- and format-shifting are generally recognized as fair uses. Public Knowledge borrows its interpretation of that legislative history from the district court decision in *Universal City Studios, Inc. v. Sony Corp.*, which examined the 1971 Sound Recording Act.[747] As Professor Nimmer has explained, however, this interpretation "does not survive careful scrutiny."[748] Contrary to Public Knowledge's interpretation, the Sound Recording Act history spoke only to the copyright status of home audio recordings under the 1909 Copyright Act—a status which was quite limited given that the 1909 Act

[743] *See, e.g.*, Joint Creators Class 8 Opp'n at 6-9 (describing disc to digital, UltraViolet, Disney Movies Anywhere, digital download, internet streaming, TV Everywhere, and other on demand services); DVD CCA/AACS LA Class 8 Opp'n at 8-10; Tr. at 121:19-21 (May 19, 2015) (Teitell, DECE/UltraViolet) (stating that the UltraViolet system is used by 20 million U.S. households).

[744] *See* Joint Creators Class 8 Opp'n at 6-9; DVD CCA/AACS LA Class 8 Opp'n at 8-10.

[745] For example, opponents provided evidence demonstrating that services including cloud-based digital rights lockers UltraViolet and Disney Movies Anywhere, disc to digital services VUDU and Flixter, and various TV Everywhere offerings have launched or experienced rapid growth since the last rulemaking. *See id.*

[746] As the Register has stated repeatedly, this rulemaking is not the appropriate forum to break new ground on the scope of fair use, or to evaluate whether an exception for private copying is sound policy. 2012 Recommendation at 163; 2003 Recommendation at 106.

[747] Public Knowledge Class 8 Supp. at 3 n.3 (citing *Universal City Studios, Inc. v. Sony Corp.*, 480 F. Supp. 429, 444-46 (1979)).

[748] 2 NIMMER ON COPYRIGHT § 8B.01[D][1][a], [b]. For example, Nimmer analyzes Register Ringer's testimony and concludes that "[f]ar from endorsing the *Sony* district court's view that the 1971 Amendment created a home recording exemption, Ms. Ringer was careful not to claim even that home recording would constitute fair use." *Id.*

did not at the time recognize copyright protection for sound recordings.[749] The cited history therefore does not support proponents' sweeping proposition that all types of space- or format-shifting are noninfringing.

Public Knowledge's interpretation of the relevant case law is equally unpersuasive. As the Register has explained previously, the *Sony* and *Diamond Multimedia* decisions upon which proponents purport to rely do not in fact address the space- and format-shifting uses proposed for these classes. As noted before, *Diamond Multimedia*, which interpreted AHRA, "did not hold that 'space-shifting' is fair use," but instead "state[d], in dicta, that 'space-shifting' of digital and analog musical recordings is a noncommercial personal use consistent with the Audio Home Recording Act."[750]

Nor did *Sony* address whether space-shifting was a fair use. The Supreme Court in *Sony* conducted its analysis solely on the basis of "time-shifting," or "record[ing] a program [one] cannot view as it is being televised [] to watch it once at a later time."[751] The Court declined to address the practice of "librarying," or maintaining long-term copies of works.[752] "Librarying," however, is clearly one of the uses contemplated by proponents here.[753]

Proponents assert that the recent *Dish* decision provides new and persuasive legal authority for the view that space- and format-shifting are noninfringing. But in the Register's view, such a reading is not justified by the facts of the *Dish* case or the opinion itself. *Dish* involved a much more circumscribed use than the uses proposed for this exemption. The Hopper Transfers service—a subscriber-based offering—included many safeguards to prevent unfettered use of the content. For instance, content obtained through the Hopper Transfers service would be deactivated if the device on which it was stored had not connected to the Dish website in the past 30 days.[754] In addition, certain programs were deleted from the set-top box once they were transferred to another device, and Dish placed limitations on the number of devices to which a work could be

[749] Nimmer also notes that "even if the *Sony* district court were right in finding a home-use exemption in the 1971 Amendment, there is no suggestion in the legislative history that the 1976 Act incorporated a similar exemption." *Id.* Instead, "it was the *judicial* doctrine of fair use developed under the 1909 Act, not any legislative directives accompanying the 1971 Amendment, that the 1976 Act adopted." *Id.* Public Knowledge's reliance upon the 1961 Copyright Office Report is similarly unpersuasive, not least because Register Kaminstein was addressing whether the public performance right should be extended to motion pictures, and not private reproduction or the technologies at issue in the current exemption.

[750] 2003 Recommendation at 130 n.234; *see also* 2012 Recommendation at 162 (same).

[751] S*ony*, 464 U.S. at 421.

[752] *Id.* at 422-23, 442; *see also* 2012 Recommendation at 162-63; 2003 Recommendation at 106.

[753] *See, e.g.*, Public Knowledge Space-Shifting Pet. at 4 (stating the desire to "to make backup copies of their movie collections in case of corrupted, lost, or stolen files"); Englander Supp. at 1.

[754] *Dish*, 2015 WL 1137593, at *6, *29.

transferred, as well as the length of time content would be available on the device.[755] In contrast, proponents request an exemption that would place works permanently "in the clear," that is, fully free of technical restrictions on further copying and distribution.

Moreover, the *Dish* court engaged in only minimal analysis of the fair use issue, reaching its conclusion in a single paragraph without discussing the statutory fair use factors (and ultimately concluding that the Hopper Transfers service in any event violated relevant contractual provisions).[756] The only support the court cited for the proposition that the space-shifting at issue was fair use was *Diamond Multimedia*.[757] As explained above, though, *Diamond Multimedia* did not address whether space-shifting was a fair use under copyright law generally; instead, it merely characterized space-shifting as a noncommercial personal use in the context of AHRA.[758]

In contrast, the recent case *Fox News Network, LLC v. TVEyes Inc.*,[759] which issued after the *Dish* opinion, confirms that courts do not accept the proposition that space-shifting as a general matter constitutes a fair use. *TVEyes* involved a video clip downloading tool offered to subscribers by a news monitoring service.[760] Noting that "[c]onvenience alone is not ground for finding fair use," the *TVEyes* court rejected defendant TVEyes' argument that offering a downloading service was "absolutely critical" to allow subscribers to view the monitored clips offline.[761] In so doing, the court cited a long line of precedent, including cases holding that the photocopying of physical journals[762] and a digital service designed to allow subscribers to access music purchased on CDs via the internet,[763] were not fair uses.

In the absence of clear supporting precedent, the fair use analysis here largely follows the 2012 analysis.[764] Under the first fair use factor, proponents are not persuasive that the purpose and character of the proposed use favors an exemption; proponents plainly seek to use works for the same entertainment purposes as were originally intended.[765] Proponents do not address the second factor, the nature of the copyrighted

---

[755] *Id.* For example, "[t]here are some types of DVR recordings that can only be transferred once (*i.e.*, HBO content), after which the original recording will be deleted from the Hopper." *Id.* at *6.

[756] *Id.* at *30-31.

[757] *Id.* at *30.

[758] *Diamond Multimedia*, 180 F.3d at 1079; *see also* 2003 Recommendation at 130 n.234.

[759] *Fox News Network, LLC v. TVEyes Inc.*, No. CV 13-5315 AKH, 2015 WL 5025274 (S.D.N.Y. Aug. 25, 2015).

[760] *See id.* at *7.

[761] *See id.* at *9.

[762] *See id.* (citing *Am. Geophysical Un. v. Texaco, Inc.*, 60 F.3d 913, 923 (2d Cir. 1994) (rejecting fair use where employees photocopied scientific journals for "personal convenience")).

[763] *See id.* at *8(citing *UMG Recordings, Inc. v. MP3.Com, Inc.*, 92 F. Supp. 2d 349, 351 (S.D.N.Y. 2000)).

[764] *See* 2012 Recommendation at 163-65; *see also* 2012 Final Rule, 77 Fed. Reg. at 65,277.

[765] *See* Public Knowledge Class 8 Supp. at 6.

work, but the Register notes that the proposals would encompass films, television programs, books, and other works that are likely to be highly creative in nature and at the core of copyright's protective purpose. Proponents are equally silent regarding the third factor, the "amount and substantiality of the portion used in relation to the copyrighted work as a whole,"[766] but the proposed exemptions are predicated on a desire to reproduce entire copyrighted works. The second and third factors thus weigh significantly against fair use.

As to the fourth factor, Public Knowledge has not offered a factual record to support its assertion that space- or format-shifting would not negatively impact the market for or value of copyrighted works.[767] By contrast, opponents submitted extensive evidence concerning existing markets for DVD and Blu-ray discs, as well as a variety of emerging internet-based distribution services.[768] Opponents assert that unfettered personal copying will harm these distribution models, some of which are specifically aimed at allowing consumers to access works already owned on physical media through online channels.[769] The burden lies with proponents to show lack of market harm. On the record as presented, the Register is unable to conclude that the proposed exemption will not negatively impact this market.

Proponent OmniQ contends that the "non-reproductive" space-shifting model it describes in its comments is a noninfringing use because the process described does not constitute reproduction under the Copyright Act.[770] The Register cannot credit OmniQ's arguments in light of its failure to establish that the technology it advocates has actually been developed. The question therefore appears to be a hypothetical one. In any event, the cases on which OmniQ seeks to rely for its assertions involve physical rather than digital copies of copyrighted works.[771] The most closely analogous case appears instead to be *Capitol Records v. ReDigi*,[772] which concluded that transferring digital files from one location to another implicates the reproduction right and is therefore infringing, even where the original copy is contemporaneously or subsequently deleted.[773]

---

[766] 17 U.S.C. § 107(3).

[767] *See* Public Knowledge Class 8 Supp. at 6-8.

[768] DVD CCA Class 8 Opp'n at 11-12; Tr. at 106:22-23 (May 19, 2015) (Williams, Joint Creators).

[769] DVD CCA Class 8 Opp'n at 12; Joint Creators Class 8 Opp'n at 5-9.

[770] OmniQ Reply at 6-8.

[771] *Id.* (citing *Théberge v. Galerie d'Art du Petit Champlain Inc.*, [2002] 2 S.C.R. 336 (Can.) (involving the physical transfer of art to canvas); *Lee v. A.R.T.*, 125 F.3d at 581 (involving the mounting of art on ceramic tiles); *C. M. Paula v. Logan*, 355 F. Supp. 189 (involving the transfer of a print from one backing to another)).

[772] *Capitol Records, LLC v. ReDigi Inc.*, 934 F. Supp. 2d 640, 648 (S.D.N.Y. 2013) (finding that because the unauthorized transfer and sale of digital music files on the internet was a reproduction under the Copyright Act, even where the original copy was deleted, neither fair use nor the first sale doctrine applied).

[773] *Id.* at 650 ("It is beside the point that the original phonorecord no longer exists. It matters only that a new phonorecord has been created."). OmniQ also argues that private performance is a noninfringing use

In sum, based on the evidentiary record in this proceeding and under current law, the Register is unable to determine that the proposed uses are noninfringing.

b. Adverse Effects

Even if the Register were to conclude that the uses here are noninfringing, proponents have not offered a sufficient record of adverse effects to warrant the granting of an exemption. Public Knowledge's principal claim is that it would be costly for consumers to re-purchase a digital version of lawfully acquired physical audiovisual works.[774] However, as the Register has previously noted, the 1201 exemption process is meant to ensure that users have access to copyrighted works; it is not meant to guarantee consumers the ability to access content through their preferred method or format.[775] Moreover, the premise of Public Knowledge's concern about costs appears somewhat misplaced. Public Knowledge suggests at several points that consumers are not purchasing DVDs but are purchasing access to the content contained on those DVDs.[776] Based on opponents' submissions, however, consumers pay lower prices for movies on DVD or Blu-ray discs than they would pay if those movies could be converted to any digital format and/or copied an unlimited number of times.[777] Assuming that is correct, then consumers purchasing DVDs or Blu-ray discs are not necessarily harmed in economic terms.[778]

Nor have proponents sufficiently demonstrated that services, including online download or streaming services, disc-to-digital services, digital rights locker systems, "TV Everywhere" or similar on-demand services, do not provide reasonable alternatives to circumvention.[779] Opponents introduced detailed evidence of a wide variety of platforms and media that can serve as alternatives to circumvention.[780] As noted above,

---

that supports an exemption. OmniQ Reply at 5. As the Register has previously noted, however, space-shifting for noninfringing private performance is insufficient grounds for an exemption if the space-shifting also requires a reproduction. *See* 2006 Recommendation at 70.

[774] *See* Public Knowledge Class 8 Supp. at 7. Class 10 petitioner Meadows did not provide written comments in response to the Office's NPRM. The potential harms outlined in the initial petition, such as the possible future bankruptcy of e-book stores, are therefore rejected as speculative due to lack of evidentiary support.

[775] 2012 Recommendation at 163; *see also Corley*, 273 F.3d at 459. Opponents also introduced evidence that, in many cases, consumers who have purchased a physical copy of a motion picture can obtain a digital copy for free or a fee depending on the service and the audiovisual work. Joint Creators Class 8 Opp'n at 6-8.

[776] Public Knowledge Class 8 Supp. at 8-9; Public Knowledge Class 8 Reply at 5-7; Tr. at 94:01-07 (May 19, 2015) (Siy, Public Knowledge).

[777] *See* DVD CCA/AACS LA Class 8 Opp'n at 4-5.

[778] *See* Tr. at 103:05-07 (May 19, 2015) (Williams, Joint Creators).

[779] Public Knowledge Class 8 Reply at 7-8.

[780] *See* DVD CCA/AACS LA Class 8 Opp'n at 9-10; Joint Creators Class 8 Opp'n at 5-9, Exhibits 1-6; Tr. at 105:06-16 (May 19, 2015) (Williams, Joint Creators) (referencing the wide availability of content on various platforms).

the record shows that these alternatives have expanded since the last rulemaking, and that such services' catalogs continue to grow. Additionally, it remains possible to access disc media through the use of peripheral devices.[781] The many alternatives suggest that the market is responding to consumer demand for the very uses proponents desire to make.[782]

Accordingly, on the present record, the Register is not persuaded that the inability to engage in the activities described by proponents is adversely affecting consumers' ability to make noninfringing uses of copyrighted works.[783]

4. NTIA Comments

As it did in the last rulemaking, in evaluating Proposed Class 8, NTIA again supports what it terms a "narrowed version" of an exemption to allow circumvention "when the disc neither contains nor is accompanied by an additional copy of the work in an alternate digital format, and when circumvention is undertaken solely in order to accomplish the noncommercial space shifting of the contained motion picture."[784] NTIA frames the exemption as an issue of consumer protection.[785] In support of its view, NTIA cites an article by scholar Pamela Samuelson maintaining that "format shifting" or "platform shifting" is "widely accepted as fair."[786]

At the same time, NTIA acknowledges that "there has been considerable debate over whether, and under what circumstances, space shifting may be considered a noninfringing use."[787] In noting that NTIA's comments may diverge from the Register's ultimate recommendation, NTIA observes that "[t]he disagreement between our two offices is reflective of a larger debate over the merits and legality of noncommercial space shifting."[788]

NTIA recognizes that the industry has created services to meet consumer demand, finding that UltraViolet specifically "enables consumers to lawfully experience works on a range of devices and formats."[789] NTIA, however, believes that "such services have not

---

[781] *Compare* Public Knowledge Class 8 Supp. at 14-15, *and* Public Knowledge Class 8 Reply at 7-8, *with* Joint Creators Class 8 Opp'n at 4-5 (disputing same).

[782] *See* Tr. at 105:06-16 (May 19, 2015) (Williams, Joint Creators).

[783] Because proponents have failed to make their case on the fundamental prerequisites to recommend an exemption, the Register sees no need to consider the statutory factors enumerated in section 1201(a)(1)(C). *See* 2012 Recommendation at 166 n.935.

[784] NTIA Letter at 32-33; *see also* 2012 Recommendation at 166 (same, for DVDs only).

[785] NTIA Letter at 29-33.

[786] *Id.* at 30 (citing Pamela Samuelson, *The Generativity of Sony v. Universal: The Intellectual Property Legacy of Justice Stevens*, 74 FORDHAM L. REV. 1831, 1866 (2006)).

[787] *Id.* at 29.

[788] *Id.* at 30.

[789] *Id.* at 31-32.

been made available with the large majority of the physical media ever sold" and are limited to those with high speed internet access.[790]

With respect to Class 10, concerning space-shifting of literary works, NTIA declines to recommend an exemption due to the lack of evidentiary submissions. Nonetheless, NTIA explains that it "is open to this type of exemption in principle."[791]

5. Conclusion and Recommendation

While the Register recognizes the continuing interest in the proposed exemptions represented in Classes 8 and 10, for the reasons discussed above, the Register is unable to recommend these classes. Based on the record presented during the proceeding, the Register cannot conclude that the space- and format-shifting activities advocated by proponents are noninfringing, or that the prohibition on circumvention has, or is likely to have, an adverse impact on noninfringing uses of the underlying works. The Register therefore declines to recommend these classes.

[790] *Id.*

[791] *Id.* at 35.

C. Proposed Class 9: Literary Works Distributed Electronically – Assistive Technologies

1. Proposal

Proposed Class 9 would allow circumvention of technological measures protecting literary works distributed in electronic form so that such works can be accessed by persons who are blind, visually impaired, or print disabled. The exemption would apply to e-books, digital textbooks, and PDF articles. The American Foundation for the Blind ("AFB"), American Council for the Blind ("ACB"), Samuelson-Glushko Technology Law & Policy Clinic at Colorado Law ("Samuelson-Glushko TLPC at Colorado Law"), and the Library Copyright Alliance ("LCA") filed petitions seeking to have the Librarian renew the exemption granted in 2012 for these purposes.[792] The NPRM described the exemption as follows:

> Proposed Class 9: This proposed class would allow circumvention of access controls on lawfully made and acquired literary works distributed electronically for purposes of accessibility for persons who are print disabled. This exemption has been requested for literary works distributed electronically, including e-books, digital textbooks, and PDF articles.[793]

Additional comments supporting this exemption were filed by the Association of American Publishers ("AAP"), Music Library Association ("MLA"), iFixit, the Free Software Foundation ("FSF"), 121AuthEnt.org, Inc., and over 1200 individuals. [794]

a. Background

E-books are books in digital formats that are distributed electronically and are downloaded by users to their personal computers or portable devices. Although a variety of sources and e-book formats are available, the three leading e-book platforms are Amazon's Kindle, Barnes & Noble's Nook, and Apple's iBooks, the last of which is an

---

[792] AFB/ACB/Samuelson-Glushko TLPC at Colorado Law ("AFB Parties") Pet. at 2; LCA Literary Works Pet. at 1. In subsequent comments, AFB Parties were joined by LCA. The 2012 exemption specifies:

> Literary works, distributed electronically, that are protected by technological measures which either prevent the enabling of read-aloud functionality or interfere with screen readers or other applications or assistive technologies in the following instances: (i) when a copy of such a work is lawfully obtained by a blind or other person with a disability, as such a person is defined in 17 U.S.C. 121; provided, however, the rights owner is remunerated, as appropriate, for the price of the mainstream copy of the work as made available to the general public through customary channels; or (ii) when such work is a nondramatic literary work, lawfully obtained and used by an authorized entity pursuant to 17 U.S.C. 121.

37 C.F.R. § 201.40(b)(1).

[793] NPRM, 79 Fed. Reg. at 73,863.

[794] *See* AAP Supp.; MLA Class 9 Supp.; FSF Class 9 Supp.; iFixit Class 9 Supp.; 121AuthEnt.org Reply; Digital Right to Repair Class 9 Supp. (1292 individuals).

application that can be used with Apple devices such as the iPhone and iPad.[795] In previous rulemaking proceedings, the Register has noted the significant role of e-books in improving accessibility for persons who are blind, visually impaired or print disabled.[796] At the same time, as the Register has also recognized, many e-books are protected by TPMs that interfere with the proper operation of assistive technologies.[797] As a result, the Librarian has adopted exemptions in previous rulemaking proceedings allowing circumvention of such technological measures.[798]

The current exemption allows for circumvention by individuals and entities that qualify for the exceptions set forth in section 121 of the Copyright Act, also known as the "Chafee Amendment." The Chafee Amendment provides that it is not an infringement of copyright "for an authorized entity to reproduce or to distribute copies or phonorecords of a previously published, nondramatic literary work if such copies or phonorecords are reproduced or distributed in specialized formats exclusively for use by blind or other persons with disabilities."[799] The Amendment defines "authorized entities" to include "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," and also provides a definition of "blind or other persons with disabilities."[800] The 2012 exemption incorporates these definitions.[801] Notably, the current exemption was designed to benefit not only blind persons or others with disabilities, but also "authorized entities" that provide services for such persons. The Register explained in 2012 that "authorized entities should enjoy an exemption to the extent required for them to carry out their work under Section 121."[802]

b. Asserted Noninfringing Uses

Class 9 proponents assert that reproducing copies in accessible formats is a noninfringing use under the Chafee Amendment, because it "allows authorized entities to create and provide copies of accessible works for use by people who are blind, visually impaired, or print disabled."[803] In addition, proponents explain that converting e-books

[795] 2012 Recommendation at 16.

[796] *See, e.g., id.*

[797] *Id.* at 23.

[798] 2012 Final Rule, 77 Fed. Reg. at 65,262-63; 2010 Final Rule, 75 Fed. Reg. at 43,837; 2006 Final Rule, 71 Fed. Reg. at 68,475. The Librarian also designated a similar class in 2003. *See* 2003 Final Rule, 68 Fed. Reg. at 62,014 ("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.'").

[799] 17 U.S.C. § 121(a).

[800] *Id.* § 121(d)(1)-(2).

[801] 2012 Recommendation at 16-17; 2012 Final Rule, 77 Fed. Reg. at 65,278.

[802] 2012 Recommendation at 24; 2012 Final Rule, 77 Fed. Reg. at 65,262.

[803] AFB Parties Supp. at 10; *see also* iFixit Class 9 Supp. at 4.

into accessible formats is an "uncontroversial" noninfringing fair use, citing the legislative history of the 1976 Copyright Act and the recent *Authors Guild, Inc. v. HathiTrust* decision as support.[804] iFixit, a supporting party, adds that the Americans with Disabilities Act ("ADA") supports the view that making copies of e-books accessible is noninfringing, because "[v]isual-impairments, including blindness, clearly fit under the ADA's definition of a disability, which is defined as 'a physical or mental impairment that substantially limits one or more major life activities of such individual,' including the act of reading."[805] Proponents also note that most of the commenters do not dispute that "making e-books accessible is an archetypical fair use."[806] Ultimately, in proponents' words, their desire is simply to "guarantee[] the right of people who are blind or visually impaired to read books."[807]

c. Asserted Adverse Effects

Class 9 proponents observe that millions of Americans are blind, visually impaired, or print disabled, including approximately 80,000-120,000 students.[808] They contend that renewal of the exemption is necessary because, "[a]lthough some improvements in accessibility have been made since the last triennial review, TPMs continue to effectively control accessibility technology's access to many e-books and other electronically distributed literary works."[809] Proponents explain that all three major e-book platform providers—Amazon, Barnes and Noble, and Apple—utilize TPMs that can affect accessibility or render an otherwise accessible e-book "completely inaccessible."[810] For example, only 28.26% of Pulitzer Prize-winning and 33.33% of Hugo Award-winning e-books of the past fifty years have Text-To-Speech ("TTS") capabilities enabled on Amazon.com.[811] iFixit pointed to a lack of accessible books as well, noting that "[o]nly 1% of published books are available in braille."[812] Moreover, proponents assert that even if the market evolves over the next three years to increase

[804] *See* AFB Parties Supp. at 11-13 (citing H.R. REP. NO. 94-1476, at 73 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5687; S. REP. NO. 94-473, at 80 (1975); *Authors Guild, Inc. v. HathiTrust*, 755 F.3d 87, 103 (2d Cir. 2014) (holding that "fair use allows the Libraries to provide full digital access to copyrighted works to their print-disabled patrons")); *see also* iFixit Class 9 Supp. at 4.

[805] iFixit Class 9 Supp. at 3-4.

[806] AFB Parties Reply at 5. Proponents also state that "the record contains no evidence suggesting that proving [sic] e-books in accessible formats is not clearly a fair use." *Id.*

[807] Tr. at 64:11-12 (May 29, 2015) (Reid, AFB Parties).

[808] AFB Parties Supp. at 14.

[809] *Id.* at 4.

[810] *Id.* at 5 (citing Sarah Hilderley, *Accessible Publishing Best Practice Guidelines for Publishers* 8 (version 4, May 2013), http://www.accessiblebooksconsortium.org/export/sites/visionip/inclusive_publishing/en/pdf/accessible_best_practice_guidelines_for_publishers.pdf ("Hilderley")).

[811] *Id.* at Apps. E-F.

[812] iFixit Class 9 Supp. at 2.

accessibility of current titles, it appears likely that many older titles will still remain inaccessible without circumvention of access controls.[813]

With respect to students who are blind, visually impaired, or print disabled, while a recent settlement agreement with the U.S. Department of Justice and Department of Education requires universities to convert e-textbooks to accessible formats, proponents note that circumvention is often necessary in order to make e-textbooks accessible for these students and is generally performed by disability services offices at universities, libraries and other institutions of higher education.[814] Proponents contend that "[p]roviding alternate format[s] for students with print disabilities puts them on a level footing with other students, and providing those materials quickly and accurately is critical to their success."[815] Proponents note, however, that the "overwhelming majority" of learning materials, including university websites, digital books, PDFs, and online research journals, remain inaccessible.[816]

Proponents further observe that other e-book formats and platforms do not provide adequate alternatives to circumvention. They explain that audiobooks—"expressive reproductions of copyrighted works that use one or more voice actors to perform the work"[817]—are inadequate "because audio versions are not available for the vast majority of e-books."[818] For example, only 150,000 audiobooks are offered by Audible.com, the leading provider of audiobooks, and only 300,000 titles—not all in audiobook format—are available through "the world's largest accessible online library for people with print disabilities."[819] By comparison, there are more than one million e-book titles offered by Amazon.com.[820] According to proponents, audiobooks are in any event inadequate because they are not necessarily navigable by page numbers and chapter titles by persons who are blind, visually impaired or print disabled, and because they are far more expensive than e-books, "costing up to three times as much."[821]

Proponents also assert that technical standards to facilitate accessibility technologies have not been comprehensively implemented in the three years since the last rulemaking. While the EPUB3 standard for e-book creation and distribution provides a host of accessibility options and was adopted by the International Digital Publishing

---

[813] *See* Tr. at 68:24-69:06 (May 29, 2015) (Band, LCA); *id.* at 69:07-13 (Reid, AFB Parties).

[814] AFB Parties Supp. at 14-15, App. A.

[815] *Id.* at App. A at ¶ 12; *see also id.* at 20-21, App. B; AFB Parties Reply at 6.

[816] AFB Parties Supp. at 14-15; *see also* AFB Parties Reply at 4 (noting that "[a]ccessing academic and technical writing is especially difficult for readers who are blind, visually impaired, or print disabled").

[817] AFB Parties Supp. at 15.

[818] *Id.*

[819] *Id.* (citing AUDIBLE, http://www.audible.com (last visited Oct. 7, 2015) and *Who We Are*, BOOKSHARE, https://www.bookshare.org/cms/about (last visited Oct. 7, 2015)).

[820] *Id.*

[821] *Id.* at 16.

Forum in 2013, it has still not been widely implemented by publishers and consequently is not considered an adequate alternative by proponents.[822] Proponents further note that "all commenters in this proceeding agreed that ePub3 and HTML 5 standards do not currently satisfy the needs of consumers who are blind, visually impaired, or print disabled."[823]

Although an e-book that is inaccessible on one platform may be accessible on another, Class 9 proponents explain that it would be "unjust to require [persons who are blind, visually impaired, or print disabled] to expend their resources on extraneous devices when they may already have an otherwise perfectly capable device," pointing in particular to the fact that nearly 8.2 million such Americans are "near or below the poverty level."[824] Proponents further note that many e-reader devices "remain extremely expensive and complex" and provide only limited accessibility features.[825] For example, proponents note that several popular e-book readers—the Kindle Paperwhite, Kindle Reader, and the Nook—do not offer TTS accessibility, while cheaper e-reader devices, such as Kobo and Sony Reader, are "totally inaccessible out of the box."[826] Proponents also explain that popular accessible devices, such as the Kindle Fire HDX 8.9, are still of only limited utility since they are locked to certain services, such as Amazon.[827]

d. Argument Under Statutory Factors

Proponents urge that the statutory factors set forth in section 1201(a)(1) support granting this exemption as well. With respect to the first factor, which addresses the general availability of copyrighted works, proponents explain that the exemption would improve the availability of accessible works for people who are blind, visually impaired, or print disabled.[828] Regarding the second factor, which considers availability for educational purposes, proponents contend that the exemption would facilitate use of works by students as well as university disability offices and specialty libraries assisting

[822] The EPUB standard is an "open standard for e-book creation and distribution . . . . [that] can be 'read' on almost all e-reader devices." Hilderley at 11 (cited in AFB Parties Supp. at 5 n.5). EPUB3 is the latest version of the EPUB standard, consisting of a file format using HTML and CSS, and provides a "host of accessibility options." *Id.* at 11-12.

[823] AFB Parties Reply at 3.

[824] AFB Parties Supp. at 17-18. AFB Parties also pointed to the NTIA's comments during the 2012 rulemaking proceeding, which stated that "[r]equiring visually impaired Americans to invest hundreds of dollars in an additional device (or even multiple additional devices), particularly when an already-owned device is technically capable of rendering literary works accessible, is not a reasonable alternative to circumvention." *Id.* at 17 (citing Letter from Lawrence E. Strickling, Assistant Secretary, NTIA, to Maria Pallante, Register of Copyrights, at 5 (Sept. 21, 2012), http://copyright.gov/1201/2012/2012_NTIA_Letter.pdf).

[825] *Id.* at 18.

[826] *Id.*

[827] *Id.* Separately, Proposed Class 12 addresses whether to adopt an exemption to allow unlocking of all-purpose tablet computers, including the Kindle Fire.

[828] *Id.* at 19-20; AFB Parties Reply at 5.

them.[829] On the third factor, proponents argue that the exemption would facilitate equal access to information for purposes of criticism, commentary, news reporting, teaching, scholarship, or research.[830] As for the fourth factor, proponents assert that the prior exemptions have had no effect on the market for the underlying copyrighted works, as the e-book market has "grown substantially since 2008 notwithstanding the exemption."[831] They further note that the AAP does not oppose an exemption in recognition that the market has not yet provided an adequate alternative to circumvention.[832]

Finally, for the fifth factor, concerning such other factors as the Librarian considers appropriate, proponents suggest that renewing an e-book accessibility exemption will serve to bring the United States into compliance with the Marrakesh Treaty to Facilitate Access to Published Works for Persons Who Are Blind, Visually Impaired or Otherwise Print Disabled ("Marrakesh Treaty") and signal the U.S.'s "commitment to equal access for people who are blind, visually impaired, or print disabled" to information.[833] The Marrakesh Treaty, which the United States helped negotiate and to which it is a signatory, creates international standards to promote the accessibility of literary and artistic works.[834] The Marrakesh Treaty requires contracting states to provide for "a limitation or exception to the right of reproduction, the right of distribution, and the right of making available to the public . . . to facilitate the availability of works in accessible format copies," and to ensure that anticircumvention laws do not prevent persons who are blind, visually impaired, or print disabled "from enjoying the limitations and exceptions provided for in this Treaty."[835] Consequently, proponents suggest that an exemption from the prohibition on circumvention in order to promote accessibility is consistent with the mandate of the Marrakesh Treaty and would put the United States on equal footing with countries that are already implementing the Treaty.[836]

---

[829] AFB Parties Supp. at 20-21; AFB Parties Reply at 6.

[830] AFB Parties Supp. at 21-22; AFB Parties Reply at 6.

[831] *See, e.g.*, AFB Parties Supp. at 23.

[832] *Id.*; AFB Parties Reply at 7; *see also* AFB Parties Reply at 4 (stating that "it is undisputed that the present-day market for books accessible to the handicapped is so insignificant that 'it is common practice in the publishing industry for authors to forego royalties for books manufactured in specialized formats for the blind'") (citing *HathiTrust*, 755 F.3d at 103).

[833] AFB Parties Reply at 7; AFB Parties Supp. at 23.

[834] *See* AFB Parties Supp. at 23; Marrakesh Treaty, June 27, 2013, *available at* http://www.wipo.int/treaties/en/text.jsp?file_id=301016. While the United States is a signatory to the Marrakesh Treaty, it has not yet ratified the Treaty. *WIPO-Administered Treaties: Notifications > Marrakesh VIP Treaty (Treaty not yet in force)*, WORLD INTELLECTUAL PROPERTY ORGANIZATION, http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&search_what=N&treaty_id=843 (last visited Oct. 7, 2015).

[835] Marrakesh Treaty arts. 4, 7; *see also* Tr. at 66:21-67:02 (May 29, 2015) (Band, LCA) ("The treaty has a provision, I believe it is Article VII, that indicates countries need to have a way for people who are blind or authorized entities have to have a way to circumvent technological protection measures in order to take advantage of any exception under the treaty.").

[836] AFB Parties Supp. at 23-24; AFB Parties Reply at 7.

2. Opposition

There was no opposition to renewing the 2012 exemption.[837] Significantly, AAP, representing book publishers, filed supportive comments indicating that it had no objection to a renewal of the existing exemption. AAP acknowledges that despite the proliferation of mobile devices used to read e-books, the market "do[es] not yet offer inherent accessibility across such platforms or in the commercially-available versions of such works for consumers with print disabilities."[838]

AAP does note, however, that it disagrees with the removal from the 2012 exemption of "the requirement . . . that circumvention [is] permitted only if all existing e-book editions of the work (including digital text editions made available by authorized entities under Section 121 of the Copyright Act) contain[] restrictive access controls."[839] At the recommendation of the Register, the 2012 exemption eliminated the condition in earlier versions of the exemption that all e-book editions be inaccessible in order for the exemption to apply.[840] AAP further opines that the Register and Librarian should "remain open to narrowing or rejecting such an exemption in the future as market conditions . . . limit the variability of accessibility capabilities across such devices and increase the commercial availability of accessible versions of such works in the marketplace."[841]

3. Discussion

The Register is sensitive to the need to ensure that access controls do not prevent persons who are blind, visually impaired, or print disabled from gaining meaningful access to books distributed in electronic formats.[842] The need for and desirability of access to such works by those with impairments—access that might otherwise be denied—present a quintessential case for an exemption to the prohibition on circumvention.

a. Noninfringing Uses

Citing the legislative history of the 1976 Copyright Act, the 1996 passage of the Chafee Amendment, the 2014 *HathiTrust* decision, and other authority, Class 9 proponents offer strong support for their claim that converting e-books into accessible formats is a noninfringing fair use.

---

[837] 121AuthEnt disagreed with AFB Parties' interpretation of *HathiTrust*, but did not oppose granting the requested exemption. 121AuthEnt Opp'n at 3-4.

[838] AAP Supp. at 1.

[839] *Id.*

[840] *See* 2012 Recommendation at 21; *see also* 2006 Final Rule, 71 Fed. Reg. at 68,475; 2003 Final Rule, 68 Fed. Reg. at 62,014.

[841] AAP Supp. at 1.

[842] *See* 2003 Recommendation at 64; 2006 Recommendation at 37; 2012 Recommendation at 24-25.

In passing the 1976 Act, Congress expressed concern for the ability of blind individuals to access copyrighted works, observing in a House Report that "the making of a single copy or phonorecord by an individual as a free service for a blind persons [sic] would properly be considered a fair use under section 107."[843] Subsequently, in 1996, Congress passed the Chafee Amendment, codified in section 121 of the Copyright Act, to "end the unintended censorship of blind individuals' access to current information" by allowing groups that produce specialized formats for persons who are blind, visually impaired, or print disabled to do so without first having to gain permission from copyright owners.[844]

As the Register noted in her 2012 Recommendation, however, "several provisions in Section 121 appear ill-suited to the digital world and could benefit from comprehensive review by Congress."[845] Subsequently, in 2014, Congress held a hearing on exceptions for the visually impaired, at which Representative Bob Goodlatte explained that "the visually impaired community has the expectation and the right to participate in our community and the copyrighted works created within it," and further observed that "[t]he technology used to access copyrighted works for the visually impaired has changed with the digital revolution."[846] In 2015 testimony before Congress, addressing areas that are ripe for legislative action, the Register reinforced Chairman Goodlatte's observation, noting that the Chafee Amendment "would benefit from immediate attention through a legislative process . . . . [so it can] better address the current needs of the visually impaired community and developments in the commercial marketplace."[847]

Additionally, since the last triennial rulemaking, the Court of Appeals for the Second Circuit in *HathiTrust* determined that providing print-disabled patrons with accessible versions of works in a library's digital archive was a fair use.[848] In *HathiTrust*, several research universities allowed Google to electronically scan the books in their collections so they could be included in a repository, the HathiTrust Digital Library ("HDL").[849] The HDL, among other uses, "allows member libraries to provide patrons with certified print disabilities access to the full text of copyrighted works" in their collections, using adaptive technologies.[850] In assessing whether this was a fair use, the

[843] H.R. REP. NO. 94-1476, at 73.

[844] 142 CONG. REC. S9764 (daily ed. Sept. 3, 1996) (statement of Sen. Chafee); *see also HathiTrust*, 755 F.3d at 102 (noting that "the Chafee Amendment illustrates Congress's intent that copyright law make appropriate accommodations for the blind and print disabled").

[845] 2012 Recommendation at 24.

[846] *Copyright Issues in Education and for the Visually Impaired: Hearing Before the Subcomm. On Courts, Intellectual Property, and the Internet of the H. Comm. on the Judiciary*, 113th Cong. 3-4 (2014) (statement of Rep. Bob Goodlatte, Chairman, H. Comm. on the Judiciary).

[847] *The Register's Perspective on Copyright Review: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 21 (2015) (statement of Maria A. Pallante, Register of Copyrights and Dir., USCO).

[848] *HathiTrust*, 755 F.3d at 101-03.

[849] *Id.* at 90.

[850] *Id.* at 91.

court emphasized that providing access to the print disabled is a favored purpose under copyright law. The court pointed in particular to the statement by the Supreme Court in in *Sony v. Universal* that "[m]aking a copy of a copyrighted work for the convenience of a blind person is expressly identified by the House Committee Report as an example of fair use, with no suggestion that anything more than a purpose to entertain or to inform need motivate the copying."[851]

In sum, the Register finds that for purposes of this rulemaking, proponents have made a compelling case that making e-books accessible to persons who are blind, visually impaired or print disabled is a noninfringing use.[852]

b. Adverse Effects

The Register finds that proponents have demonstrated that all major e-book platforms employ TPMs that to some degree hinder accessibility software, and that only a fraction of e-book titles are currently available in accessible formats. Proponents have demonstrated that popular e-reader devices still have substantial limitations—for example, in lacking built-in accessibility features such as TTS capabilities—or are completely inaccessible out of the box. In addition, as demonstrated by proponents, alternatives, such as audiobook formats, are insufficient alternatives due to limited availability or functionalities. The Register also notes that AAP concedes that the current market does not yet meet the accessibility needs of consumers with print disabilities;[853] a great many e-books are not available in accessible formats, and older titles are even less likely to be available. Proponents have also demonstrated that a significant number of learning materials are inaccessible to blind, visually impaired and print disabled students. For these reasons, the Register believes that proponents have amply demonstrated that the presence of TPMs on electronically distributed literary works is likely to have an adverse impact on noninfringing activities in the upcoming three-year period.

c. Statutory Factors

Out of the five statutory factors set forth in section 1201(a)(1) that the Librarian and the Register are to consider, the Register finds that all five factors strongly favor the exemption. First, an exemption to facilitate assistive technologies enhances the availability for use of copyrighted works because it increases the number of works that may be accessed by people who are blind, visually impaired, or print disabled.[854] Second, proponents have established that the exemption will facilitate the use of works for non-profit educational purposes, including the efforts of university disability offices and specialty libraries to provide accessible versions of e-books, thus "help[ing] afford all

[851] *Id.* at 101-102; *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 455 n.40 (1984).

[852] *See, e.g.*, 2006 Recommendation at 38 (noting that "[t]here was also no dispute that rendering an ebook accessible to visually impaired persons is a noninfringing activity"); 2003 Recommendation at 70.

[853] AAP Supp. at 1.

[854] *See, e.g.*, AFB Parties Supp. at 19-20, Apps. E-F; AFB Parties Reply at 5-6.

citizens equal access to education, education technologies, and democratic participation."[855] Third, it will promote access to works by all for purposes of research and criticism. And fourth, there is no evidence that it will undermine the value of or market for e-books, as that market has grown substantially in recent years despite the existence of earlier exemptions.

Finally, the statute also permits the Librarian to consider "such other factors" as may be appropriate.[856] As proponents note, an exemption to promote accessibility would be consistent with the mandate of the Marrakesh Treaty, which the United States helped negotiate and to which it is a signatory.[857] As is globally recognized and as the Register noted in her 2012 Recommendation, an exception to promote accessibility "is not merely a matter of convenience, but is instead intended to enable individuals who are blind or visually impaired to have meaningful access to the same content that individuals without such impairments are able to perceive."[858]

4. NTIA Comments

NTIA recommends renewing the current exemption allowing people who are blind, visually impaired, or print disabled, as well as the authorized entities that serve them, to circumvent TPMs that prevent or interfere with the use of assistive technologies with e-books. NTIA notes that the Librarian has granted an exemption for this particular purpose since 2003, and finds that the evidence in the record shows that the state of accessibility of literary works in electronic format is not substantially different than it was three years ago.[859] NTIA states that many Americans are adversely affected when they cannot use assistive devices to gain access to e-books, and finds that the record contains clear and specific examples of the many ways disabled users and authorized entities are utilizing this exemption as intended and thus making literary works more accessible with assistive technologies.[860] NTIA therefore supports renewing the current exemption, without change.[861]

As explained above, the Register also finds that this exemption should be renewed in its current form.

5. Conclusion and Recommendation

Class 9 proponents have demonstrated that individuals who are blind, visually impaired, or print disabled are significantly disadvantaged with respect to obtaining

[855] *See, e.g.*, AFB Parties Supp. at 21-22; AFB Parties Reply at 6.

[856] 17 U.S.C. § 1201(a)(1)(C)(v).

[857] AFB Parties Supp. at 23.

[858] 2012 Recommendation at 22.

[859] NTIA Letter at 34.

[860] *Id.* at 34-35.

[861] *Id.* at 35.

accessible e-book content because the platforms and devices on which e-books are consumed incorporate TPMs that inhibit the use of assistive technologies. They have further established that the facilitation of accessible formats has been recognized by Congress and the courts to be a noninfringing fair use. There was no opposition to renewing the exemption in its current form.

The Register therefore recommends an exemption in the form requested to permit circumvention of TPMs on e-books to permit the use of assistive technologies. Like the existing exemption, the recommended exemption references section 121 so that the intended beneficiaries of section 121 are able to benefit from the waiver on circumvention. Accordingly, the Register recommends that the following class of works be exempt from the prohibition on circumvention for the next three years:[862]

> **Literary works, distributed electronically, that are protected by technological measures that either prevent the enabling of read-aloud functionality or interfere with screen readers or other applications or assistive technologies,**
>
> **(i) When a copy of such a work is lawfully obtained by a blind or other person with a disability, as such a person is defined in 17 U.S.C. 121; provided, however, that the rights owner is remunerated, as appropriate, for the price of the mainstream copy of the work as made available to the general public through customary channels, or**
>
> **(ii) When such work is a nondramatic literary work, lawfully obtained and used by an authorized entity pursuant to 17 U.S.C. 121.**

[862] As with the 2012 Recommendation, the recommended class has been fashioned with reference to section 121.

D. Proposed Classes 11 to 15: Computer Programs That Enable Devices To Connect to a Wireless Network That Offers Telecommunications and/or Information Services ("Unlocking")

1. Proposals

Proposed Classes 11 through 15 would allow circumvention of access controls on wireless devices such as cellphones and all-purpose tablet computers to allow them to connect to the network of a different mobile wireless carrier.[863] This process is commonly known as "unlocking."[864] Wireless carriers typically lock wireless devices to their networks when they have subsidized the cost of a device at the time of purchase; carriers recoup that subsidy through wireless service charges paid by the purchaser.[865] The purchaser often also makes a contractual commitment to use the device on the carrier's network (or to pay a termination fee),[866] although that is not necessarily true for prepaid wireless services, as discussed below.

The Register recommended, and the Librarian adopted, exemptions permitting unlocking of wireless telephone handsets (referred to for purposes of this exemption as "cellphones") in 2006,[867] 2010,[868] and 2012.[869] Additionally, in 2012, the Register declined to recommend a broader exemption for "tablets" or for all "wireless devices" because the record in that rulemaking was "devoid of any evidence" to support the existence of adverse effects caused by TPMs preventing unlocking of such devices.[870]

The 2012 version of the exemption was limited to cellphones obtained on or before January 26, 2013.[871] In 2014, however, Congress passed the Unlocking Act,

---

[863] These exemptions are relevant only to devices that are locked to cellular networks operated by commercial mobile radio and data services like Verizon Wireless, AT&T, Sprint, and T-Mobile (referred to here as "wireless carriers"), using protocols such as CDMA, GSM, HSPA+, and LTE. Consistent with the Unlocking Consumer Choice and Wireless Competition Act ("Unlocking Act"), these networks are referred to here as "wireless telecommunications networks." *See* Unlocking Act, Pub. L. No. 113–144, § 2(e), 128 Stat. 1751, 1752 (2014) (defining the term). No party in this proceeding has claimed that the concept of unlocking is relevant to other wireless communications technologies, such as those using the IEEE 802.11 standard employed in Wi-Fi routers, the Bluetooth standard, ANT wireless network technology, or mesh networks. *See* NPRM, 79 Fed. Reg. at 73,864 n.40 (inviting comment on this point).

[864] The Register notes that although the terms "firmware" and "software" are variously used throughout this Recommendation, both are "computer programs" within the meaning of the Copyright Act. *See* 17 U.S.C. § 101 (definition of "computer program").

[865] TracFone Opp'n Comments at 2.

[866] *See, e.g.*, Consumers Union Class 11 Supp. at 14.

[867] 2006 Recommendation at 42-53; 2006 Final Rule, 71 Fed. Reg. at 68,477.

[868] 2010 Recommendation at 163; 2010 Final Rule, 75 Fed. Reg. at 43,839.

[869] 2012 Recommendation at 99-100; 2012 Final Rule, 77 Fed. Reg. at 65,264-66.

[870] *See* 2012 Recommendation at 99 & n.545.

[871] 2012 Final Rule, 77 Fed. Reg. at 65,264 (sun-setting the exemption 90 days after the effective date of the rule, October 28, 2012, in light of the availability of unlocked phones).

reinstating the unlocking exemption for cellphones adopted in 2010, which lacked such a limitation.[872] In that same Act, Congress also instructed the Librarian to review any future proposal for a cellphone unlocking exemption according to the usual process in this triennial rulemaking, as well as to consider in this rulemaking whether to "extend" the cellphone unlocking exemption "to include any other category of wireless devices in addition to wireless telephone handsets."[873]

In the Unlocking Act, Congress defined, on a permanent basis, the categories of persons and entities that could take advantage of the exemption. In particular, Congress specified that the circumvention permitted under the reinstated 2010 exemption, as well as any future exemptions to permit cellphones or other wireless devices to connect to wireless telecommunications networks, could be initiated by the owner of the handset or device, by another person at the direction of the owner, or by "a provider of commercial mobile radio or a commercial mobile data service" (*e.g.*, a wireless carrier) to enable such owner or a family member to connect to a wireless network when authorized by the network operator.[874]

Notably, the unlocking exemptions granted in 2010 and 2012 specified that only the owner of the copy of the computer program on a cellphone could pursue circumvention.[875] That is because proponents in those prior rulemakings relied principally on section 117(a)(1), which authorizes the "owner" of a copy of a computer program to make or authorize the making of another copy or adaptation of that program; they did not invoke fair use.[876] Accordingly, when recommending adoption of the cellphone unlocking exemptions, the Register relied on section 117(a)(1), and imported that provision's requirement that the person engaging in circumvention be the owner of the computer program.[877] The Unlocking Act, however, suggests Congress's intent that any unlocking exemption allow the owner of the *device* to engage in circumvention, without regard to whether the software is owned by or licensed to the owner of the

[872] Unlocking Act § 2(a). *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Wireless Telephone Handsets, 79 Fed. Reg. 50,552, 50,554 (Aug. 25, 2014).

[873] Unlocking Act § 2(b).

[874] *Id.* § 2(c); H.R. REP. NO. 113-356, at 8 (2014).

[875] *See* 2012 Final Rule, 77 Fed. Reg. at 65,278; 2010 Final Rule, 75 Fed. Reg. at 43,839. The cellphone unlocking exemption granted in 2006 did not specify the persons entitled to engage in circumvention, or the precise legal ground on which unlocking was determined to likely involve noninfringing uses. 2006 Final Rule, 71 Fed. Reg. at 68,480; 2006 Recommendation 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 noninfringing activity by the user.").

[876] 2012 Recommendation at 83; 2010 Recommendation at 120 & n.412.

[877] 2010 Recommendation at 167 ("[B]ecause 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.'"); *see also* 2012 Recommendation at 89-93, 100.

device.[878] In this regard, as discussed below, proponents in this rulemaking for the first time invoke fair use, in addition to section 117(a)(1).

Consistent with Congress's directive in the Unlocking Act, the Copyright Office invited proposals to continue an unlocking exemption for wireless telephone handsets and/or to extend the exemption to other categories of wireless devices. The petitions received generally asked for continuation of the current cellphone unlocking exemption, and extension of that exemption to new categories of devices. In the NPRM, the Office grouped the petitions into five distinct classes based on the type of device at issue, described as follows:

> Proposed Class 11: This proposed class would allow the unlocking of wireless telephone handsets. "Wireless telephone handsets" includes all mobile telephones including feature phones, smart phones, and "phablets" that are used for two-way voice communication.[879]

Petitions proposing an unlocking exemption for cellphones were filed by Consumers Union,[880] the Competitive Carriers Association ("CCA"),[881] the Institute of Scrap Recycling Industries ("ISRI"),[882] Pymatuning Communications ("Pymatuning"),[883] and

---

[878] Unlocking Act § 2(c).

[879] NPRM, 79 Fed. Reg. at 73,864.

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

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

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

[883] Pymatuning's proposed regulatory language reads as follows: "Computer programs, in the form of firmware or software, that enable used wireless telephone handsets and other used wireless

the Rural Wireless Association ("RWA").[884] Additional comments supporting this exemption were filed by Catherine Gellis and the Digital Age Defense project ("Gellis/Digital Age Defense"), eBay, Inc. and Gazelle, Inc. ("eBay/Gazelle"), Free Software Foundation ("FSF"), iFixit, and over 2300 individuals.[885]

> Proposed Class 12: This proposed class would allow the unlocking of all-purpose tablet computers. This class would encompass devices such as the Apple iPad, Microsoft Surface, Amazon Kindle Fire, and Samsung Galaxy Tab, but would exclude specialized devices such as dedicated e-book readers and dedicated handheld gaming devices.[886]

Petitions proposing an unlocking exemption for all-purpose tablet computers were filed by Consumers Union,[887] CCA,[888] ISRI,[889] Pymatuning,[890] and RWA.[891] As reflected in

---

telecommunications devices to connect to a wireless telecommunications network, when circumvention is initiated by the owner of the copy of the computer program solely in order to connect to a wireless telecommunications network and access to the network is authorized by the operator of the network." Pymatuning Pet. at 2.

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

[885] Gellis/Digital Age Defense Class 11 Supp.; eBay/Gazelle Supp.; FSF Class 11 Supp.; iFixit Class 11 Supp.; Mervin Rosario Supp.; Digital Right to Repair Class 11 Supp. (2304 individuals); Digital Right to Repair Class 11 Reply (268 individuals).

[886] NPRM, 79 Fed. Reg. at 73,865.

[887] Consumers Union sought a tablet unlocking exemption as part of its cellphone unlocking petition. Consumers Union Pet. at 2-3 (''Consumers Union's proposed exemption accordingly includes all hand-held mobile wireless devices that are used for essentially the same functions and in the same manner as wireless telephone handsets, including tablets.'').

[888] CCA's proposed regulatory language reads as follows: "Computer programs, in the form of firmware or software, or data used by firmware or software, that enable all-purpose tablet computers to connect to a wireless network that offers telecommunications and/or information services, when circumvention is initiated by the owner of the device, or by another person at the direction of the owner of the device, in order to connect to a wireless network that offers telecommunications and/or information services, and access to the network is authorized by the operator of the network." CCA Tablet Unlocking Pet. at 1-2.

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

[890] Pymatuning sought a tablet unlocking exemption as part of its cellphone unlocking petition. Pymatuning Pet. at 2 (stating that because ''the justifications underlying the [Unlocking] Act also apply to

the proposal, the petitions were limited to "all-purpose" tablet computers—that is, tablet computers that can run a wide variety of programs—as opposed to dedicated devices like e-book readers or media players. Comments supporting this exemption were also filed by Gellis/Digital Age Defense, FSF, iFixit, and over 2300 individuals.[892]

> Proposed Class 13: This proposed class would allow the unlocking of mobile connectivity devices. "Mobile connectivity devices" are devices that allow users to connect to a mobile data network through either a direct connection or the creation of a local Wi-Fi network created by the device. The category includes mobile hotspots and removable wireless broadband modems.[893]

Petitions proposing an exemption for mobile connectivity devices were filed by CCA[894] and RWA.[895] Comments supporting this exemption were also filed by Gellis/Digital Age Defense, FSF, and nearly 1900 individuals.[896]

---

all portable computers, tablets and other types of devices that communicate via wireless telecommunications networks, and that are often locked much the same as wireless telephone handsets, Pymatuning requests that the scope of 'handsets' be clarified to include all such wireless telecommunications devices'').

[891] RWA's proposal would "allow for the circumvention of the technological measures that control access to all purpose tablet computer ('Tablet') software and firmware to allow the owner of a lawfully acquired Tablet, or a person designated by the owner of the lawfully acquired Tablet, to modify the device's software and firmware so that the wireless device may be used on a technologically compatible wireless network of the customer's choosing, and when the connection to the network is authorized by the operator of the network." RWA Tablet Unlocking Pet. at 1-2.

[892] Gellis/Digital Age Defense Class 12 Supp.; FSF Class 12 Supp.; iFixit Class 12 Supp.; Digital Right to Repair Class 12 Supp. (2309 individuals).

[893] NPRM, 79 Fed. Reg. at 73,865.

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

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

> Proposed Class 14: This proposed class would allow the unlocking of wearable wireless devices. "Wearable wireless devices" include all wireless devices that are designed to be worn on the body, including smart watches, fitness devices, and health monitoring devices.[897]

Petitions proposing an exemption for wearable wireless devices were filed by CCA[898] and RWA.[899] Comments supporting this exemption were also filed by Gellis/Digital Age Defense, FSF and over 1600 individuals.[900]

> Proposed Class 15: This proposed class would allow the unlocking of all wireless "consumer machines," including smart meters, appliances, and precision-guided commercial equipment.[901]

The petition proposing a wide-ranging exemption for all wireless "consumer machines" was filed by CCA.[902] As the Copyright Office noted in the NPRM, the request is for a "broad, open-ended exemption for all 'consumer machines'—or 'the "Internet of Things"'—which would encompass a diverse range of devices and equipment."[903] In its

---

[896] Gellis/Digital Age Defense Class 13 Supp.; FSF Class 13 Supp.; Digital Right to Repair Class 13 Supp. (1895 individuals). SAE International, Vehicle Electrical System Security Committee ("SAE VESS") filed comments neither in support nor opposition to the proposed exemption. SAE VESS Class 13 Supp.

[897] NPRM, 79 Fed. Reg. at 73,865.

[898] CCA addressed what it called "connected wearables" in the course of its broad catch-all proposal, the remainder of which is addressed in Proposed Class 15. *See* CCA Connected Wearables and Consumer Machines Unlocking Pet. at 1-2.

[899] RWA's proposed exemption would "allow for the circumvention of the technological measures that control access to wearable mobile wireless device ('Wearable Wireless Device') software and firmware to allow the owner of a lawfully acquired Wearable Wireless Device, or a person designated by the owner of the lawfully acquired Wearable Wireless Device, to modify the device's software and firmware so that the Wearable Wireless Device may be used on a technologically compatible wireless network of the customer's choosing, and when the connection to the network is authorized by the operator of the network." RWA Wearable Wireless Devices Unlocking Pet. at 1-2. RWA explains that "[a] Wearable Wireless Device is a wearable Internet-connected, voice and touch screen enabled, mobile wireless computing device that is designed to be worn on the body, including but not limited to a smart watch." *Id.* at 2 n.3.

[900] Gellis/Digital Age Defense Class 14 Supp.; FSF Class 14 Supp.; Digital Right to Repair Class 14 Supp. (1632 individuals).

[901] NPRM, 79 Fed. Reg. at 73,866.

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

[903] NPRM, 79 Fed. Reg. at 73,866.

opening comments, CCA confirmed this understanding, urging the Office to define the exemption as encompassing "any 'smart' device that utilizes a data connection to connect to the Internet or to interact with other smart devices."[904] Supporting comments were filed by Gellis/Digital Age Defense, FSF, iFixit, and over 1500 individuals.[905]

Because the proposed unlocking exemptions involve many overlapping factual and legal issues, Proposed Classes 11 through 15 are to some degree addressed collectively.

a. Background

i. Proposed Classes 11 to 14

The devices encompassed by Proposed Classes 11 to 14 (cellphones, tablets, mobile connectivity devices, and consumer wearables such as smartwatches) employ one or more known TPMs, including subscriber identity module ("SIM") card locks,[906] service provider code ("SPC") locks,[907] system operator code ("SOC") locks,[908] and band order locks.[909] Consumers Union notes, however, that "technological advances could create new measures that function in the same way."[910] Unlocking can be accomplished in a variety of ways. In some cases, unlocking can occur without having to circumvent any access control by entering in a model- or device-specific code to provide access to the relevant carrier settings in the phone software; this approach, however, may require

[904] CCA Class 15 Supp. at 2.

[905] Gellis/Digital Age Defense Class 15 Supp.; FSF Class 15 Supp.; iFixit Class 15 Supp.; Digital Right to Repair Class 15 Supp. (1589 individuals).

[906] SIM cards "store information used by a mobile device to identify and authenticate itself on a wireless network." Consumers Union Class 11 Supp. at 5. A SIM lock is software that "causes the device reject any SIM card it has not been programmed to recognize, namely SIM cards that would connect to other wireless networks." *Id.*; *see also* ISRI Class 12 Supp. at 4 (noting that SIM locks are used for tablets); CCA Class 13 Supp. at 3 (same for mobile hotspots); CCA Class 14 Supp. at 4 (same for wearable devices).

[907] SPC locks are used by phones using the code-division-multiple-access standard. ISRI Class 11 Supp. at 4. The SPC is a unique number generated using the device's electronic serial number and an algorithm specific to a particular wireless carrier; thus, unless a new code is obtained "the user is blocked from programming the device to work on another network." *Id.*; *see also* Consumers Union Class 12 Supp. at 6 (noting that SPC locks are used for tablets); CCA Class 13 Supp. at 3 (same for mobile hotspots); CCA Class 14 Supp. at 4 (same for wearable devices).

[908] SOCs are "code numbers, associated with particular carriers, that prevent mobile devices from connecting to wireless networks not identified by the codes." Consumers Union Class 11 Supp. at 6; *see also* ISRI Class 12 Supp. at 4 (noting that SOC locks are used on tablets); CCA Class 13 Supp. at 3 (same for mobile hotspots); CCA Class 14 Supp. at 4 (same for wearable devices).

[909] A band order lock "restricts mobile devices to using the wireless communications radio frequencies controlled by a particular carrier." Consumers Union Class 11 Supp. at 6; *see also* ISRI Class 12 Supp. at 4 (noting that band order locks are used for tablets); CCA Class 13 Supp. at 3 (same for mobile hotspots); CCA Class 14 Supp. at 4 (same for wearable devices).

[910] Consumers Union Class 11 Supp. at 5.

the assistance of the carrier or device manufacturer.[911] Absent such assistance, unlocking a phone requires circumvention of an access control. According to ISRI, circumvention generally involves running software that exploits security defects in the device to "modif[y] a variable or replace a short piece of code" on the device's operating system.[912]

An issue dividing proponents to some extent is whether the Class 11 or Class 12 exemptions should cover only "used" cellphones and tablets. The current cellphone unlocking exemption (as reinstated by Congress in the Unlocking Act) extends only to "used" phones.[913] Some proponents of Classes 11 and 12, namely Consumers Union and eBay/Gazelle, call for elimination of that limitation for cellphones and tablets.[914] Other proponents of Classes 11 and 12, however, namely, ISRI and CCA, expressly request an exemption limited to "used" devices.[915] ISRI specifically proposes that "used" be defined for purposes of the proposed exemption as a device "that has been lawfully acquired and activated on the wireless telecommunications network of a carrier."[916] With respect to devices potentially to be covered under Classes 13, 14, and 15, no participant seemed to be seeking an exemption for unused devices.[917]

Another issue in this rulemaking is the extent to which so-called "bulk" unlocking can and should be accommodated in any unlocking exemption.[918] A number of legitimate charities and commercial enterprises (such as bulk recyclers of cellphones and other devices represented by ISRI) obtain used devices from consumers and unlock them in large quantities for the purposes of resale or redistribution.[919] But there is also an unlawful form of large-scale unlocking that involves the bulk purchase of unused handsets that have been offered for sale at subsidized prices by prepaid wireless carriers, and then unlocking and reselling those unlocked handsets for a profit. This concern is described in greater detail in the course of addressing opponent TracFone, Inc.'s ("TracFone's") comments below. The 2010 rulemaking addressed this issue; the Register explained that by requiring that the cellphones be "used," the 2010 exemption was designed to prevent the "illegal trafficking of mobile phones."[920]

---

[911] *See, e.g.*, ISRI Class 11 Supp. at 5.

[912] *Id.*

[913] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Wireless Telephone Handsets, 79 Fed. Reg. at 50,553-54.

[914] Consumers Union Class 11 Supp. at 1; eBay/Gazelle Supp. at 5.

[915] *See, e.g.*, ISRI Class 11 Reply at 5 (emphasizing that its proposal was designed to encompass only used devices); CCA/TracFone Reply at 2 (agreeing to joint proposal limited to used phones).

[916] *See, e.g.*, ISRI Class 11 Supp. at 14.

[917] *See* Tr. at 18:24-25 (May 21, 2015) (Wiens, iFixit) (agreeing that it "would be reasonable" to limit unlocking exemptions to used devices).

[918] NPRM, 79 Fed. Reg. at 73,864.

[919] *See, e.g.*, ISRI Class 11 Supp. at 12-14.

[920] 2010 Recommendation at 169. An earlier version of the Unlocking Act included language that might have been construed as prohibiting all bulk unlocking for purposes of resale. *See* Unlocking Consumer

ii. Proposed Class 15: Consumer Machines

As the Office described it in the NPRM, Class 15 is a "broad, open-ended exemption for all consumer machines—or the Internet of Things—which would encompass a diverse range of devices and equipment."[921] In the NPRM, the Office noted its concern that "it may be difficult to build an adequate administrative record for this exemption in light of the fact-bound analysis required by section 1201(a)(1)."[922] For instance, the Office noted that CCA referred to "precision-guided commercial equipment" in its petition, but "provide[d] no explanation as to the kind of equipment to which it refers."[923] The Office accordingly encouraged CCA and other proponents "to provide targeted argument and evidence that would allow the Office to narrow this category appropriately."[924]

CCA filed the sole substantive comment in support of the exemption, and failed to further define the kinds of "smart" devices the exemption would cover beyond those already encompassed by Classes 11 through 14, let alone the types of TPMs used by such devices or the methods of circumvention. Indeed, it is not apparent from the record whether such devices even exist. For instance, while CCA suggested that smart power meters would be encompassed by the proposal,[925] evidence at the public hearing (at which CCA did not participate) indicates that smart meters generally do *not* have mobile data (*e.g.*, 3G/4G) connections, rendering the concept of unlocking irrelevant to that type of device.[926]

Choice and Wireless Competition Act, H.R. 1123, 113th Cong. § 2(c)(2) (2014) ("Nothing in this subsection shall be construed to permit the unlocking of wireless handsets or other wireless devices, for the purpose of bulk resale, or to authorize the Librarian of Congress to authorize circumvention for such purpose[.]"). That provision was added to the House bill after it passed out of committee, and was a matter of substantial debate on the House floor. *See* 160 CONG REC. H1904-13 (daily ed. Feb. 25, 2014). The bulk unlocking ban was not included in the Senate version of the bill, which was the one enacted into law. *See* Unlocking Consumer Choice and Wireless Competition Act, S.517, 113th Cong (2014).

[921] NPRM, 79 Fed. Reg. at 73,866 (internal quotations omitted).

[922] *Id.*

[923] *Id.*

[924] *Id.*

[925] CCA Class 15 Supp. at 9.

[926] *See* Tr. at 28:03-06 (May 21, 2015) (Wiens, iFixit) ("[W]e're talking about connections to cellular networks. Smart meters don't connect to the cellular network. So smart meters establish their own mesh network.").

b. Asserted Noninfringing Uses

To support the claim that unlocking constitutes a noninfringing use of the device software, proponents of the unlocking classes advance three general arguments across all of the unlocking classes.[927]

First, they note that in many instances, unlocking a wireless device does not implicate any of the copyright owner's exclusive rights under the Copyright Act. CCA explains, for example, that cellphones are "typically" unlocked "by changing the variables in certain handset memory locations and updating the preferred roaming list ('PRL') to make the handset compatible with a new network."[928] According to proponents, changing such variables in software does not involve reproduction of a copyrighted work or result in a derivative work.[929]

Second, as in past rulemakings, proponents of the unlocking classes argue that, to the extent unlocking implicates any of the exclusive rights of the copyright owner, the activity falls within the limitation on exclusive rights in computer programs set forth in section 117(a)(1).[930] That provision allows the "owner" of a copy of a computer program to make or authorize the making of another copy or adaptation of that program created "as an essential step in the utilization of the computer program in conjunction with a machine and that [] is used in no other manner."[931] Proponents contend that the owners of wireless devices are the owners of the underlying device software under either of the two leading cases on software ownership[932]—*Krause v. Titleserv, Inc.*[933] and *Vernor v. Autodesk, Inc.*[934] Proponents also argue that unlocking is an "essential step" for using the device software with a wireless service provider of a consumer's choice, and note that the Register reached the same conclusion in 2012.[935]

---

[927] Consumers Union also urges a point not made by other proponents: that the software that enables connectivity between a mobile device and a wireless network "likely falls outside the Copyright Act's protection for expressive works" because it is "functional" in nature. Consumers Union Class 11 Supp. at 10-11. At the same time, Consumers Union acknowledges that "mobile device manufacturers and wireless carriers have not conceded this point" and that, given the uncertainty about the merits of this argument, "a DMCA exemption is still necessary." *Id.* at 11. In light of that acknowledgment, and the other bases for recommending an exemption, it is unnecessary to address this point further, except to observe that computer programs are protectable under the Copyright Act. *See* 17 U.S.C. § 101 (definition of "computer program").

[928] CCA Class 11 Supp. at 3.

[929] Consumers Union Class 11 Supp. at 11-12; ISRI Class 12 Supp. at 6-7; CCA Class 13 Supp. at 4; CCA Class 14 Supp. at 5; CCA Class 15 Supp. at 5.

[930] *See, e.g.*, CCA Class 11 Supp. at 4-7; ISRI Class 12 Supp. at 9-12.

[931] 17 U.S.C. § 117(a).

[932] *See, e.g.*, CCA Class 11 Supp. at 5-7; ISRI Class 12 Supp. at 10-11.

[933] 402 F.3d 119 (2d Cir. 2005).

[934] 621 F.3d 1102 (9th Cir. 2010).

[935] *See, e.g.*, CCA Class 12 Supp. at 5; ISRI Class 12 Supp. at 12.

Third, for the first time, proponents of the unlocking classes also argue that any reproductions or derivative works created in the process of unlocking would constitute fair use under section 107.[936] ISRI urges that each of the four fair use factors supports this view. First, ISRI argues that the purpose of the use is to make purely functional adjustments to the software to enable interoperability with a different wireless carrier, and that such uses have been recognized by courts to be fair.[937] In addition, ISRI, representing bulk recyclers, asserts that any commercial aspect of bulk unlocking is "fairly attenuated from the unlocking use of the . . . software and does not involve selling copies or derivative works of it other than as a tiny component of a used device."[938] With respect to the second factor, ISRI notes that the nature of the software at issue is highly functional, and is thus entitled to less protection than more creative works.[939] On the third factor, ISRI asserts that the amount of the work used is small, because unlocking only changes those portions of the software that help connect the phone to a particular carriers' network, leaving the rest intact.[940] On the last factor, both ISRI and CCA maintain that unlocking has no appreciable adverse effect on the market for or value of the device software.[941] Indeed, they urge that "the ability to lawfully unlock mobile devices likely increases the value of those devices (including the embedded software)" because it allows them to be resold more easily to new users.[942]

Some proponents also rely on the Unlocking Act to reinforce their argument that unlocking is a noninfringing activity. Relying upon the Senate report for the Unlocking Act, Consumers Union asserts that the Act "embodies Congress's view that unlocking a mobile device is a legitimate non-infringing use."[943] ISRI similarly asserts that the Unlocking Act "should properly be read as Congress' determination that the unlocking that Petitioner seeks here should be lawful, whatever the precise legal ownership status of software . . . on the unlocked devices."[944] ISRI points to the legislative history of the Unlocking Act as evidence that Congress wanted to accommodate bulk unlocking. ISRI

---

[936] *See, e.g.*, ISRI Class 11 Supp. at 7-9; CCA Class 12 Supp. at 4.

[937] *See, e.g.*, ISRI Class 12 Supp. at 7 (citing *Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1520 (9th Cir. 1992) and *Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596, 602-603 (9th Cir. 2000)).

[938] *Id.* at 8.

[939] *See, e.g.*, *id.* (citing *Sega*, 977 F.2d at 1524).

[940] *See, e.g.*, *id.* ("[T]he changes are limited to the portion of the software that prevents unlocking—while the vast remainder of the software remains undisturbed and allows the device to continue functioning as intended.").

[941] *See, e.g.*, *id.* at 9; CCA Class 11 Supp. at 4.

[942] ISRI Class 12 Supp. at 9; *see also* CCA Class 11 Supp. at 4 ("[T]he market for and value of the copyrighted work actually increases, as it allows the handset to be transferred on the secondary market more easily and to a broader array of buyers.").

[943] Consumers Union Class 11 Supp. at 10; *see* S. REP. NO. 113-212, at 6 (2014) ("Unlike many other situations where an exemption from the circumvention prohibition may be sought or granted, unlocking a cell phone to connect to a wireless network typically does not facilitate copyright infringement.").

[944] ISRI Class 12 Supp. at 12.

notes that an earlier version of the bill included language that could have been construed as prohibiting bulk unlocking for the purpose of resale, but that this language was stripped out before the Unlocking Act was passed into law.[945]

c. Asserted Adverse Effects

Although proponents assert some of the same adverse effects across all the unlocking classes, there are sufficient differences in the factual record to warrant a separate discussion of each class.

i. Proposed Class 11: Wireless Telephone Handsets

Class 11 proponents assert that wireless carriers commonly install TPMs on cellphone software that prevent consumers from using the cellphone on another carrier's network in order to enforce the consumer's commitment to use the phone on the original carrier's network.[946] Proponents note, however, that once consumers have satisfied their commitments to the carriers, the TPMs remain in place. They assert that, absent a continued exemption, the prohibition on circumvention of those TPMs will lead to several adverse effects. First, CCA and Consumers Union assert that the prohibition impedes consumers' ability to switch their existing cellphones to the wireless carrier of their choice. Instead, consumers must continue with a wireless carrier they may be dissatisfied with, or spend sometimes significant sums to purchase a new phone that can function on the network of their desired wireless carrier.[947] CCA notes consumers also invest sometimes substantial sums on music, apps, and peripheral equipment that is tied to their existing cellphone, and that these investments might be lost if the consumer is forced to purchase a new phone from their desired carrier.[948] In addition to these harms to individual consumers, Consumers Union suggests that the prohibition on cellphone unlocking has broader anti-competitive effects: by "ensur[ing] that customers cannot easily be lured away by a competitor," the prohibition "dampens competitive pressure on carriers to improve prices and terms of service."[949]

Second, Class 11 proponents point to evidence that locked cellphones have significantly lower resale value than unlocked ones, disadvantaging consumers who want to resell their used locked phones and businesses that resell used phones.[950] Gazelle, a leading reseller of used cellphones, explains that "because much of the market for eligible iPhones, particularly AT&T phones, is overseas, Gazelle cannot obtain as high a price for resale of a locked phone as it can for resale of the same phone when it has been or can be

[945] *See* ISRI Class 11 Supp. at 14 & n.61 (citing Unlocking Consumer Choice and Wireless Competition Act, H.R. 1123 § 2(c)(2)).

[946] *See* Consumers Union Class 11 Supp. at 4-5, 13-14; eBay/Gazelle Supp. at 2.

[947] CCA Class 11 Supp. at 9-10; Consumers Union Class 11 Supp. at 13-14.

[948] CCA Class 11 Supp. at 9.

[949] Consumers Union Class 11 Supp. at 14

[950] *Id.* at 15-16; CCA Class 11 Supp. at 12.

unlocked."[951] As a result, "Gazelle cannot make as valuable an offer to a consumer for an eligible locked AT&T phone as it can for that phone when it is unlocked *or* when Gazelle is confident that it can unlock that phone, or have it unlocked, on behalf of the phone's legitimate *seller*."[952] Proponent ISRI similarly provides evidence that locked cellphones are resold at a substantial discount compared to unlocked phones, making it more difficult for legitimate resellers to operate.[953]

Third, Consumers Union points to environmental harms that flow from the abandonment of functional locked cellphones that could be reused on a different network if they could be unlocked. It asserts that "restrictions on unlocking turn perfectly functional equipment into environmental waste" because "[t]he decrease in usefulness makes it more likely that consumers will simply discard their old devices, [or] that they will end up gathering dust in a drawer, . . . eventually slowly deteriorating in a landfill."[954]

Proponents also addressed two possible alternatives to circumvention, finding that neither mitigates the adverse effects of the inability to engage in unlocking.

First, a number of wireless carriers, including the four largest national carriers, have voluntarily adopted policies based on a "Consumer Code for Wireless Service" established by CTIA-The Wireless Association, under which they have agreed to help consumers unlock their cellphones under specified conditions.[955] For prepaid phones, carriers have agreed to unlock the devices "no later than one year after initial activation, consistent with reasonable time, payment or usage requirements."[956] For non-prepaid phones, carriers have agreed to unlock the phone, or provide the necessary information to unlock the phone, "after the fulfillment of the applicable postpaid service contract, device financing plan, or payment of applicable early termination fee."[957]

Class 11 proponents assert, however, that these voluntary policies fall short in several respects. Proponents note that they are voluntary, and could be revoked or changed by the carriers unilaterally.[958] CCA also points to the Senate report for the Unlocking Act,[959] which acknowledged that there were "circumstances in which

---

[951] eBay/Gazelle Supp. at 7 (declaration of Chris Sullivan, President & CEO, Gazelle).

[952] *Id.* (emphasis in original).

[953] ISRI Class 11 Supp. at 17 (noting a twenty-five dollar price drop in cellphones after the cellphone unlocking exemption lapsed in 2013).

[954] Consumers Union Class 11 Supp. at 17.

[955] *See Consumer Code for Wireless Service*, CTIA-THE WIRELESS ASSOCIATION, http://www.ctia.org/policy-initiatives/voluntary-guidelines/consumer-code-for-wireless-service (last visited Oct. 7, 2015).

[956] *Id.*

[957] *Id.*

[958] Consumers Union Class 11 Supp. at 17; ISRI Class 11 Supp. at 19.

[959] CCA Class 11 Supp. at 7.

additional avenues for unlocking may be preferable over attempting to unlock through the carrier."[960] The Senate report noted, for example, that "some carriers require customers to bring their devices to the carrier's physical store to have them unlocked," but that "[f]or those customers who do not live near the carrier's retail location . . . this requirement may prevent them from being able to get their devices unlocked."[961] Proponents highlight other difficulties that consumers may face when asking carriers to unlock their phones. Consumers Union notes that T-Mobile "require[s] that the customer provide proof of purchase for the device," and that T-Mobile and AT&T impose certain device eligibility requirements.[962] CCA also notes unlocking a device may require a code provided by the original equipment manufacturer ("OEM"), but that OEMs are not signatories to the agreement and could decline to provide that code.[963] In addition, ISRI explains that the carriers' voluntary policies do not cover entities that engage in bulk unlocking.[964]

Second, proponents reject the availability of new unlocked cellphones as a viable alternative to circumvention. Although ISRI acknowledges that "[a]n increasing number of wireless devices . . . are now being sold unlocked," it observes that there are "millions of devices previously sold that are currently locked," and more "that will continue to be sold locked."[965] ISRI thus argues that the existence of unlocked phones "does nothing to eliminate the loss of choice and value caused by the inability to unlock the millions of recent-model devices that have already been sold to consumers and could be resold on the secondary market."[966] CCA further notes that "a consumer may not find her desired handset as one of the unlocked options," and that this is a particular concern for consumers with disabilities, who may have very specific device requirements.[967]

As noted above, Consumers Union and eBay/Gazelle also argue that consumers will suffer if the existing exemption is not extended to new devices still under contract. eBay/Gazelle did not explain what uses would be permitted by allowing such phones to be unlocked under the exemption.[968] For its part, Consumers Union points only to the possibility that a consumer might want to give a new subsidized phone received from a wireless carrier to a friend or family member who uses a different wireless carrier, while continuing to use their old phone on their existing wireless carrier (thus satisfying the service commitment).[969] But, at the public hearing on Proposed Classes 11 and 12,

[960] S. REP. NO. 113-212, at 2.

[961] *Id.*

[962] Consumers Union Class 11 Supp. at 18.

[963] CCA Class 11 Supp. at 8.

[964] ISRI Class 11 Supp. at 16.

[965] *Id.* at 20.

[966] *Id.*; *see also* eBay/Gazelle Supp. at 5.

[967] CCA Class 11 Supp. at 9.

[968] *See* eBay/Gazelle Supp. at 5.

[969] Consumers Union Class 11 Supp. at 1.

Consumers Union acknowledged that this scenario was not the focus of the requested exemption.[970] Moreover, Consumers Union conceded that a wireless carrier was unlikely to allow a consumer to leave a store with a subsidized cellphone that was not connected to that carrier's wireless network.[971]

ii. Proposed Class 12: All-Purpose Tablets

An initial question concerning the need for an exemption for tablet devices is the extent to which tablets are locked to particular wireless carriers. To begin with, unlike cellphones, many tablets are sold only with Wi-Fi capabilities and cannot connect to a wireless telecommunications network (*e.g.*, a 3G/4G network). Even tablets that can connect to such networks are frequently sold unlocked.[972] For instance, iFixit, a supporter of the tablet unlocking exemption, concedes that the highly popular Apple iPad is generally sold unlocked.[973] Nonetheless, Class 12 proponents provide some evidence that tablets purchased through wireless carriers may be locked. Consumers Union submitted the unlocking policies for the major carriers, some of which acknowledge the locking of tablets to carrier networks.[974] ISRI, representing electronics recyclers, reports that "increasingly tablet computers are being sold that connect to wireless communications networks and are locked to a particular carrier."[975]

Class 12 proponents make the same points as Class 11 proponents with respect to the adverse effects of the unlocking ban for tablets—that the prohibition on circumvention impedes consumers' ability to choose their preferred wireless carriers, harms the resale value of used devices, and creates environmental harms by encouraging disposal rather than reuse of devices.[976] They also reiterate that the potential alternative

---

[970] Tr. at 224:19-21 (May 26, 2015) (Slover, Consumers Union) ("We think, as a practical matter, most of the phones that are going to be involved here are going to be used phones.").

[971] *Id.* at 259:11-18 (Charlesworth, USCO; Slover, Consumers Union).

[972] By comparison, the wireless device reseller Gazelle reports that 74% of all of the smartphones it received in 2014 were locked to a carrier. eBay/Gazelle Supp. at 7 (declaration of Chris Sullivan, President & CEO, Gazelle).

[973] Tr. at 12:13-15 (May 21, 2015) (Wiens, iFixit); CCA Class 12 Supp. at 7 (noting that "iOS alone accounts for nearly one-third of the tablet market"); *see also* iPad Q&A, EVERYIPAD.COM (Nov. 25, 2014), http://www.everymac.com/systems/apple/ipad/ipad-faq/ipad-design-info-font-where-to-buy-unlocked.html (stating that "iPad models equipped with wireless mobile data connectivity (3G or 4G+LTE), regardless of generation, are 'unlocked' and not tied to a carrier in the United States"). Some iPads are sold with SIM cards that can only be used on a particular carrier, but the device can be moved to another carrier simply by swapping out the SIM card. *See* Kevin C. Tofel, *Fenced In: That Unlocked Apple IPad SIM Gets Locked When Activated on AT&T*, GIGAOM (Oct. 24, 2014), https://gigaom.com/2014/10/24/fenced-in-that-unlocked-apple-ipad-sim-gets-locked-when-activated-on-att.

[974] *See* Consumers Union Class 12 Supp. at Exhibit G (unlocking policy for Sprint) ("Many Sprint phones or tablets . . . have been programmed with a master subsidy lock . . . that locks the device . . . ."); *id.* at Exhibit H (unlocking policy for AT&T covering both wireless phones and tablets).

[975] ISRI Class 12 Supp. at 3.

[976] *See, e.g.*, Consumers Union Class 12 Supp. at 13-18; CCA Class 12 Supp. at 7-8.

avenues to circumvention are inadequate—that the wireless carriers' voluntary unlocking policies and the availability of unlocked tablets do not adequately mitigate the adverse effects of the unlocking ban.[977]

iii. Proposed Class 13: Mobile Connectivity Devices

Class 13 proponents observe that mobile connectivity devices, such as mobile hotspots and removable wireless broadband modems, are used by "[m]illions of Americans"[978] and that such devices are expected to "gain in popularity" over the next three years.[979] Proponents also provide evidence that wireless carriers are locking mobile connectivity devices to their networks. CCA explains that "AT&T, one of the largest wireless carriers in the nation, makes their locking policy for all devices clear, explicitly stating that they place software locks on mobile hotspots."[980]

With respect to the adverse effects caused by the prohibition on circumvention, CCA, as the sole proponent to file detailed comments for this class in response to the NPRM, focuses on the fact that the prohibition on circumvention impedes consumers' ability to choose their preferred wireless carrier.[981] CCA identifies the additional concern that carriers' voluntary unlocking policies are not a viable alternative to circumvention for mobile connectivity devices because they are limited to phones and tablets and "do[] not include mobile hotspots."[982]

iv. Proposed Class 14: Wearable Computing Devices

Concerning the proposed class of "wearable computing devices," a question highlighted by the Office in the NPRM is the extent to which such devices—which would include smartphones, fitness devices, and smart glasses—have dedicated connections to wireless telecommunications networks (*e.g.*, 3G/4G connections) and are locked to a particular wireless carrier. CCA agrees with the Office that "most smart watches, and most if not all fitness and health monitoring devices, do not employ mobile telecommunications or data networks . . . for wireless connections, but instead use either Wi-Fi to connect to a local wireless network, or Bluetooth or ANT technologies to connect to a smartphone or computer."[983] But CCA and other Class 14 proponents observe that wearable devices with freestanding mobile data connections are beginning to emerge in the marketplace. Proponents note that the Samsung Gear S smartwatch, which features a dedicated 3G connection, was introduced last year; moreover, AT&T sells a locked version of that watch for a subsidized price in exchange for a service

[977] *See, e.g.*, Consumers Union Class 12 Supp. at 17-19; CCA Class 12 Supp. at 8-10.

[978] CCA Class 13 Supp. at 7.

[979] RWA Mobile Hotspots Unlocking Pet. at 4.

[980] CCA Class 13 Supp. at 7.

[981] *Id.*

[982] *Id.*

[983] CCA Class 14 Supp. at 3 (quoting NPRM, 79 Fed. Reg. at 73,866).

commitment.[984] CCA asserts, moreover, that this trend is likely to continue, explaining that "[a]s batteries and radio transmitters become ever-smaller, it is highly likely that in the very near term such devices will no longer be dependent on Wi-Fi or smartphones for their data connection."[985]

With respect to the adverse effects caused by the prohibition on circumvention, Class 14 proponents reiterate the points made by proponents in the other unlocking classes—that the prohibition on circumvention impedes consumers' ability to choose their preferred wireless carriers, harms resale value, and creates environmental harms.[986] As with the mobile hotspots addressed in Class 13, CCA again points out that the carriers' voluntary unlocking policies do not include wearable devices.[987]

v. Proposed Class 15: Consumer Machines

As noted above, CCA fails to provide any specific information about the types of devices encompassed by the proposed exemption for "consumer machines," or the types of adverse effects faced by users of such devices. For instance, CCA makes a passing reference to Verizon's "Smart Cities solutions."[988] It appears that Verizon markets this technology to municipalities as a means of adding wireless monitoring and control capabilities to water and sewage systems, public lighting, traffic controls, and other elements of municipal infrastructure.[989] But CCA offers no evidence that a municipality using such a system would want to switch wireless carriers, or even that such systems contain TPMs preventing municipalities from doing so.

d. Argument Under Statutory Factors

Proponents of all of the unlocking classes make the same basic arguments under the 1201(a)(1) statutory factors. First, with respect to the availability for use of copyrighted works, proponents note that by allowing used devices to be unlocked, the

[984] *Id.* at 3-4; Tr. at 16:24-17:02 (May 21, 2015); *see also Samsung Gear S-Black*, AT&T, http://www.att.com/devices/samsung/gear-s.html (last visited Oct. 7, 2015) ("*Samsung Gear S-Black*") (offering the Samsung Gear S for $99.99 with a two year contract, and $299.99 without a contract).

[985] CCA Class 14 Supp. at 4.

[986] *Id.* at 7 ("The most clear, and most immediate, adverse effect . . . is to prevent consumers from easily switching their wearable devices to the competing network of their choice."); eBay Class 14 Reply at 1 (noting that unlocked smartwatches have "higher values in the resale market"); Tr. at 17:23-18:08 (May 21, 2015) (Wiens, iFixit) (noting that a month after the introduction of the Samsung Galaxy Gear, an electronics recycling facility had 200 of them).

[987] CCA Class 14 Supp. at 8.

[988] CCA Class 15 Supp. at 3.

[989] *See Smart Cities*, VERIZON, http://www.verizonenterprise.com/solutions/connected-machines/smart-cities (last visited Oct. 7, 2015).

devices (and the copyrighted software embedded within the devices) will remain usable for longer periods of time, and will contribute to a more robust resale market.[990]

Second, some proponents argue that an unlocking exemption will make copyrighted works more available for nonprofit archival, preservation, and educational purposes. For example, Consumers Union notes that "[c]onsumers increasingly use mobile devices as educational tools both in and out of the classroom."[991] In contrast, in its submissions supporting the exemptions in Classes 11 and 12, ISRI suggests that the prohibition on circumvention "does not directly bear on" these types of activities in the context of the proposed unlocking exemptions.[992]

Third, some proponents argue that the exemption will promote criticism, comment, news reporting, teaching, scholarship, and research. For example, Consumers Union argues that granting the exemption "would make it easier for more consumers to obtain a mobile device affordably and get the benefits of the digital news revolution."[993] In contrast, ISRI again indicates that the prohibition on circumvention "does not directly bear on the . . . activities" listed in the third statutory factor."[994]

Fourth, proponents argue that permitting circumvention will have no adverse effect on the market for or value of wireless device software. Several proponents note that during the period in which the prior and current unlocking exemptions have been in effect, sales of wireless devices increased rapidly.[995] Indeed, as noted above, some proponents assert that granting the exemption in fact enhances the value of the devices (and presumably the software embedded within them), because unlocked phones can be resold for significantly higher sums than locked phones.[996]

Under the fifth statutory factor, which allows for consideration of such other factors as the Librarian considers appropriate, many proponents urge that granting the exemption would increase consumer choice and competition among wireless carriers and devices.[997]

---

[990] *See, e.g.*, CCA Class 11 Supp. at 10-11; ISRI Class 12 Supp. at 23.

[991] Consumers Union Class 11 Supp. at 21.

[992] ISRI Class 11 Supp. at 23.

[993] Consumers Union Class 11 Supp. at 22.

[994] ISRI Class 11 Supp. at 23.

[995] ISRI Class 12 Supp. at 22 (citing cellphone industry research); CCA Class 11 Supp. at 12 (citing research showing growth in the number of devices connected to wireless networks).

[996] *See, e.g.*, Consumers Union Class 11 Supp. at 23; ISRI Class 12 Supp. at 23-24.

[997] *See, e.g.*, ISRI Class 11 Supp. at 24; Consumers Union Class 11 Supp. at 14-15.

2. Opposition

a. Proposed Class 11: Wireless Telephone Handsets

Although prepaid wireless carrier TracFone nominally filed comments in opposition to the cellphone unlocking exemption,[998] at bottom it is not opposed to a narrow "pro-consumer" exemption.[999]

TracFone's chief concern is that any exemption exclude illegitimate phone trafficking that could damage its prepaid wireless service. In a prepaid service, customers do not pay usage charges for service for the preceding month, as in a typical postpaid service, but instead pay for a set amount of usage in advance. TracFone explains that it and other prepaid wireless carriers "subsidize and discount the retail price of their phones to make them affordable to consumers, often reducing their prices significantly below the wholesale cost."[1000] For instance, TracFone offers "smartphones with prices as low as $9.99."[1001] According to TracFone, prepaid carriers "recoup their subsidy investments over time, through charges their customers pay to use the subsidized phones on their networks."[1002] Unlike a traditional postpaid wireless service, prepaid wireless services do not typically require customers to make a fixed service commitment at the time of purchase.[1003]

This business model makes prepaid services particularly susceptible to illegitimate phone trafficking. TracFone explains that "service providers in foreign countries do not subsidize wireless handsets," and phone traffickers "buy phones here and export them overseas for profit—stealing the subsidies that were intended to benefit legitimate American consumers."[1004] TracFone notes that to mitigate this problem, it "protects its phones with locks that prevent traffickers from modifying its copyrighted software embedded in each phone in order to use the phone on foreign networks," and that it has aggressively filed suits under the DMCA against phone traffickers.[1005]

---

[998] *See* TracFone Opp'n at 9-17.

[999] *Id.* at 3 (stressing that it supports "a pro-consumer exemption to 17 U.S.C. § 1201 that permits legitimate consumers acting in good faith to unlock their wireless telephone handsets, so long as the exemption expressly excludes any provision that could be exploited by traffickers to steal subsidies and harm consumers").

[1000] *Id.* at 2.

[1001] *Id.*

[1002] *Id.*

[1003] *See id.* at 2, 5.

[1004] *Id.* at 2.

[1005] *Id.*

Opposing any exemption that "could be construed to immunize illegal activities of phone traffickers," TracFone has proposed an alternative exemption with particularized limitations to address the trafficking concern:[1006]

> Computer programs, in the form of firmware or software, or data used by firmware or software, that enable wireless devices to connect to a different wireless network than the network to which it was previously locked (the "Original Network"), when initiated by the owner of the device (the "Owner"), or by another person at the direction of the Owner, but only if: (a) all legal obligations to the Original Network service provider associated with the provision of any subsidy, discount, installment plan, lease, rebate or other incentive program (collectively, "Subsidy") have been satisfied by or waived for the Owner; (b) the device was not obtained by theft or fraud; and (c) such unlocking is not for any unlawful purpose, including, but not limited to, obtaining unauthorized access to a wireless network or profiting from the Subsidy.[1007]

In a joint reply filed with TracFone, proponent CCA agreed to support this narrower proposal.[1008] Notwithstanding the specific formulation above, however, TracFone indicates that its concerns could instead be addressed by "official comments in the record making clear that the intent of the exemption is not to benefit traffickers."[1009]

Several other Class 11 proponents oppose the specific language of TracFone's alternative proposal.[1010] But notably, each of these proponents concurs that any exemption should exclude the sort of trafficking of which TracFone complains. Consumers Union emphasizes that "'subsidy thieves' or phone traffickers that concern TracFone are not included in the exemption."[1011] Similarly, ISRI states that it "condemns illegal trafficking of new phones."[1012] Both Consumers Union and ISRI, however, contend that their proposals, as well as the current exemption, already exclude such illegal trafficking without the added conditions proposed by TracFone. ISRI notes that under the existing exemption, TracFone has "made extensive use of lawsuits against illegal phone traffickers raising a variety of legal claims, including the DMCA, to protect

---

[1006] *Id.* at 3-4.

[1007] CCA/TracFone Reply at 2.

[1008] *Id.* at 1-2.

[1009] TracFone Opp'n at 7.

[1010] *See* Consumers Union Class 11 Reply at 2-3; ISRI Class 11 Reply at 1-2.

[1011] Consumers Union Class 11 Reply at 5 ("Consumers Union's proposed exemption strikes the right balance in both protecting the rights of consumers and protecting parties like TracFone from illegal phone trafficking.").

[1012] ISRI Class 11 Reply at 2; *see also id.* at 5 (quoting TracFone Opp'n at 3("The exemption proposed by ISRI, while applying to both direct consumers and legitimate bulk recyclers, is carefully crafted to 'expressly exclude any provision that could be exploited by traffickers' and it effectively achieves that exclusion.")).

its subsidies."[1013] Thus, Consumers Union and ISRI claim that the modifications to the proposed exemption offered by TracFone are unnecessary to address TracFone's concerns, and would merely create confusion about the scope of the exemption.[1014]

b. Proposed Class 12: All-Purpose Tablets

There is no opposition to the proposed unlocking exemption for all-purpose tablet computers.

c. Proposed Class 13: Mobile Connectivity Devices

There is no opposition to the proposed unlocking exemption to the extent it covers the sort of portable mobile connectivity devices addressed in the NPRM—hotspots and removable wireless broadband modems. The Alliance of Automobile Manufacturers ("Auto Alliance") and General Motors LLC ("GM"), however, filed opposition comments in Class 13 solely to stress that any exemption should exclude mobile connectivity devices embedded in motor vehicles.[1015] As GM explains, many automobiles come equipped with in-vehicle telematics and communications systems, including Wi-Fi hotspots, that rely on wireless telecommunications networks.[1016] In the case of GM's OnStar service, the wireless carrier is AT&T, and the OnStar system is locked to AT&T's network.[1017]

The record at the hearing demonstrated that, circumvention aside, there are currently no apparent means for users to unlock in-vehicle telematics and communications systems to connect to alternative networks, and no proponent expressed a desire to do so. As a GM representative explained at the public hearing, because the OnStar service "is designed to be used in the event that the vehicle crashes or there is an emergency," the company "build[s] the OnStar module into the vehicle . . . in a way to enhance the survivability of the module if there is a dramatic crash event."[1018] To achieve this result, the module "is buried as deep into the car as it can possibly be put," and the SIM card that allows the module to connect to AT&T's wireless network is "basically hard wired into the module."[1019] Indeed, a supporter of the proposed unlocking exemptions confirmed that understanding during the public hearing, testifying that it is not possible to switch networks without destroying your car, or perhaps "in the process[]

[1013] *Id.* at 6.

[1014] Consumers Union Class 11 Reply at 2; ISRI Class 11 Reply at 8-9.

[1015] Auto Alliance Class 13 Opp'n at 1; GM Class 13 Opp'n at 3.

[1016] GM Class 13 Opp'n at 4; Tr. at 21:13-25 (May 21, 2015) (Charlesworth, USCO; Damle, USCO; Lightsey, GM). Exemptions to allow access to vehicle telematics and communications systems are discussed and considered in Proposed Classes 21 and 22.

[1017] Tr. at 22:10-11 (May 21, 2015) (Lightsey, GM).

[1018] *Id.* at 22:13-21 (Lightsey, GM).

[1019] *Id.* at 23:21-23, 24:02-03 (Lightsey, GM).

of destroying your car."[1020] GM's representative further testified that even if it were physically possible to select a different wireless carrier, the OnStar system would not operate because "[a]ll of the protocols and the data that is pulled out of the vehicle [are] engineered to work through a specific carrier."[1021]

d. Proposed Class 14: Wearable Computing Devices

There is no opposition to the proposed unlocking exemption for wearable computing devices.

e. Proposed Class 15: Consumer Machines

Auto Alliance opposes the exemption for "consumer machines," as it "could inadvertently sweep cars and trucks into the exemption."[1022] Auto Alliance notes that the term "consumer machine" is "ill-defined" and turns on "the applicability of a completely undefined term, 'smart device.'"[1023] Otherwise, there is no specific opposition to this class.

3. Discussion

a. Noninfringing Uses

i. Proposed Classes 11 to 14

The Register concludes that proponents have provided sufficient support for the claim that unlocking a wireless device is likely to be a noninfringing use in the case of Classes 11 through 14—that is, cellphones, all-purpose tablet computers, portable mobile connectivity devices, and wearable computing devices. As discussed below, the record was too sparse to reach a similar conclusion with respect to "consumer machines" (Class 15).

At the outset, the Register notes that Congress, in the legislative history of the Unlocking Act, stated that "[u]nlike many other situations where an exemption from the circumvention prohibition may be sought or granted, unlocking a cell phone to connect to a wireless network typically does not facilitate copyright infringement."[1024] Although this statement from the legislative history is not in and of itself dispositive of the issue, Congress's opinion is relevant to the analysis.

The Register concludes that there are three grounds on which unlocking is likely to be considered a noninfringing activity.

[1020] *Id.* at 39:06-13 (Charlesworth, USCO; Wiens, iFixit).

[1021] *Id.* at 24:15-24 (Charlesworth, USCO; Lightsey, GM).

[1022] Auto Alliance Class 15 Opp'n at 1.

[1023] *Id.*

[1024] S. REP. NO. 113-212, at 5.

First, as proponents note, there are likely to be a significant number of cases where unlocking a device does not require the user to reproduce the device software or create a derivative work. Proponents provide evidence that cellphones and other wireless devices can be unlocked and transferred to an alternative network simply by changing variables in the cellphone's software in a manner that is intended by the software's creator.[1025] Thus, as the Register concluded in 2010 and again in 2012, in such cases, "the elimination and insertion of codes or digits . . . cannot be considered an infringement of the computer program controlling the device," because such "minor alterations of data . . . do not implicate any of the exclusive rights of copyright owners."[1026] Indeed, it may be that such a system does not function as a TPM at all, thus obviating the need for an exemption.[1027]

Second, as the Register has concluded in past rulemakings, even where unlocking a cellphone requires reproduction or creation of a derivative work, those acts may be noninfringing under section 117.[1028] The applicability of section 117 requires consideration of two questions: whether the owner of a wireless device is also an "owner" of the embedded operating system software, and whether creating a new copy or adaptation of that software is an "essential step" in utilization of the software with the wireless device.

In past rulemaking proceedings, the Register has reviewed case law governing the determination of ownership of a software copy for purposes of section 117 when formal title is lacking and/or a license imposes restrictions on the use of the computer program, and has concluded that application of the law can be unclear in some contexts.[1029] The Register observed that while *Vernor v. Autodesk, Inc.*[1030] and *Krause v. Titleserv, Inc.*[1031]

[1025] For instance, cellphone manufacturers design their software to work with a "preferred roaming list" that is provided by the wireless carrier, and lists the frequencies and systems that the device can connect to. *See* Jerry Hildenbrand, *What is a PRL? [Android A to Z]*, ANDROID CENTRAL (Jan. 30, 2014), http://www.androidcentral.com/what-prl-android-z. CCA notes that connecting a device to an alternative network requires replacing that preferred roaming list with one for the new wireless carrier. CCA Class 11 Supp. at 3.

[1026] 2010 Recommendation at 134; 2012 Recommendation at 90.

[1027] *See Lexmark Int'l v. Static Control Components, Inc.*, 387 F.3d 522, 546-47 (6th Cir. 2004) (concluding that section 1201(a)(1) did not apply "where the access-control measure left the literal code or text of the computer program or data freely readable").

[1028] Section 1201(f), which permits reverse engineering of computer programs for purposes of enabling interoperability with other programs, was not raised as a potential avenue to permit circumvention. In any event, that provision would not cover the full range of activities in question; among other things, circumvention here is not done to enable interoperability of "an independently created computer program with other programs," 17 U.S.C. § 1201(f)(1), but to allow a device to connect to an alternate wireless network.

[1029] *See* 2010 Recommendation at 90 (noting that "the law relating to who is the owner of a copy of a computer program under [s]ection 117 is in flux"); *see also* 2012 Recommendation at 92 ("The Register concludes that the state of the law remains unclear."); 2010 Recommendation at 129, 132.

[1030] 621 F.3d 1102.

may provide some useful guidance in this area, they are "controlling precedent in only two circuits and are inconsistent in their approach."[1032]

In *Krause*, the Second Circuit held that formal title was not necessary to demonstrate ownership under section 117, and that courts should instead look to a range of factors to determine "whether the party exercises sufficient incidents of ownership over a copy of the program to be sensibly considered the owner of the copy."[1033] These factors include: (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.[1034] By contrast, in *Vernor*, the Ninth Circuit held that "a software user is a licensee rather than an owner of a copy where the copyright owner (1) specifies that the user is granted a license; (2) significantly restricts the user's ability to transfer the software; and (3) imposes notable use restrictions."[1035] These tests remain the two dominant approaches to the question of whether software is owned or licensed.

The record contains some evidence to support the conclusion that the owner of a wireless device—whether a consumer or a bulk recycler—should be considered the owner of the software on that device for purposes of section 117. CCA notes that a number of factors set forth in *Krause* favor the conclusion that wireless device owners own the software that runs the device: the copy of the software is stored on property owned by the user, namely the cellphone or other wireless device; device owners have the right to use the programs indefinitely on those devices; and device owners have the right to discard or destroy the device (along with the copy of the software) at any time.[1036] CCA reaches a similar conclusion under the *Vernor* analysis, noting that device manufacturers and wireless carriers do not impose "notable use restrictions."[1037]

Thus, as the Register concluded with respect to cellphones in 2012, the record compels a finding that it is likely that "some subset of wireless customers . . . is entitled

---

[1031] 402 F.3d 119.

[1032] 2012 Recommendation at 92.

[1033] *Krause*, 402 F.3d at 124.

[1034] *Id.*

[1035] *Vernor*, 621 F.3d at 1111.

[1036] CCA Class 11 Supp. at 6.

[1037] *Id.* at 6-7. Indeed, for cellphones and tablets encompassed by Classes 11 and 12, CCA presents evidence that two major mobile operating systems (Apple iOS 8.1 and Windows Phone 7) expressly permit the transfer of the software to a third party in connection with the sale of a device. *Id.* at 7.

to exercise the Section 117 privilege."[1038] In this regard, it is worth noting that while previous cellphone exemptions—including the existing provision[1039]—have identified the owner of the copy of the computer program on a cellphone as the person entitled to engage in unlocking, as discussed above, the Unlocking Act demonstrates Congress's intent that device owners be entitled to engage in circumvention independent of the question of legal ownership of device software.[1040]

The record further establishes that reproduction or adaptation of the work is likely to constitute an "essential step" in the operation of the cellphone or other wireless device. A wireless device such as a cellphone or mobile hotspot can fulfill its function only when connected to a wireless service. It thus follows that if modifications to device software are necessary to make that device operate with a wireless carrier of the user's choice, those modifications can be considered an essential step in the use of the device.[1041]

Third, the Register concludes, as a matter of first impression, that unlocking as a general matter is also likely to be a fair use. The fair use analysis here is in many respects analogous to the reasoning that has led the Register to conclude in past rulemakings that "jailbreaking" of smartphones is likely to be fair use.[1042]

The first fair use factor examines the purpose and character of the use. As proponents note, the purpose of the use here is to make functional adjustments to the device software to enable the operation of a device on the wireless network of the user's choice. Courts have held that enabling interoperability with other software is favored under the first factor,[1043] and the logic of those cases can reasonably be extended to uses that enable interoperability of a device with a specific wireless network. Although such a use may not be "transformative" in that the software is used for the same essential purpose—to operate the device—a lack of transformativeness does not necessarily preclude a finding of fair use. The Register has previously concluded in the course of recommending an exemption for "jailbreaking" of smartphones that even if use of the copyrighted device software is considered nontransformative, the first factor may nonetheless favor fair use where the purpose and character of the use is "noncommercial

[1038] 2012 Recommendation at 93.

[1039] 37 C.F.R. § 201.40(c).

[1040] *See* Unlocking Act § 2(c) (providing that circumvention "may be initiated by the *owner of any such handset or other device*" (emphasis added)).

[1041] *See* 2012 Recommendation at 93 ("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 consumer. 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.").

[1042] *See, e.g.*, *id.* at 72-74 (citing 2010 Recommendation at 92-93).

[1043] *See Connectix*, 203 F.3d at 607-608; *Sega*, 977 F.2d at 1522-23.

and personal" and it enhances an owner's ability to make use of a device "for the purpose for which [it was] intended."[1044]

That said, while unlocking may represent a personal, noncommercial activity for an individual consumer, the proposed exemption would also encompass commercial uses as well—namely, unlocking to facilitate resale of used devices. The Supreme Court has held, however, that commerciality alone does not defeat a finding of fair use.[1045] Moreover, as noted, interoperability is favored under the law. Additionally, Congress seems to have recognized that bulk resale activities can be legitimate in declining to exclude them from the Unlocking Act. Overall, while the first factor is somewhat mixed, the Register finds on this record that it tends to support a finding of fair use.

The second fair use factor—the nature of the copyrighted work—weighs strongly in favor of such a finding. The works at issue, software used to connect wireless devices to wireless networks, are highly functional. They are thus outside the "core of intended copyright protection."[1046]

With respect to the third fair use factor, which considers the amount of the work used, proponents assert that unlocking requires changes only to limited parts of the device's operating system, and that the remainder remains intact.[1047] But to the extent the changes being made to the device's operating system require significant copying of software or result in a derivative work, a substantial portion of the original is being used. This arguably renders the third factor unfavorable to a fair use finding. But in this context—where the use is necessary to engage an otherwise benign activity—the factor is entitled to only modest weight. This approach is consistent with the Register's reasoning in granting jailbreaking exemptions for smartphones in prior proceedings.[1048]

Finally, under the fourth fair use factor, concerning the effect on the market for or value of the copyrighted work—often considered to be the most important consideration—the record establishes that the market for mobile device software is not likely to be harmed by the unlocking of used cellphones. In the time the existing and prior cellphone exemptions have been in effect, the market for cellphones (including the embedded computer programs) has expanded rapidly.[1049] Except in the case of prepaid cellphones, no opponent has suggested that the market for software used to operate

---

[1044] 2012 Recommendation at 74 (referring to 2010 Recommendation at 92-93).

[1045] *See, e.g.*, *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 586 (1994).

[1046] *Id.* at 584-85; *see also Sega*, 977 F.2d at 1524.

[1047] *See, e.g.*, ISRI Class 11 Supp. at 8.

[1048] 2012 Recommendation at 74 (footnote omitted) ("Those engaged in jailbreaking use only that which is necessary to engage in the activity, which is often *de minimis*, rendering the third factor potentially unfavorable, but nevertheless of minimal consequence."); *see also Sega*, 977 F.3d at 1526-27 ("[W]here the ultimate (as opposed to direct) use is as limited as it was here, the [third fair use] factor is of very little weight.").

[1049] *See* ISRI Class 11 Supp. at 23.

cellphones or other wireless devices would be harmed by allowing those devices to be unlocked. Indeed, there is evidence that unlocked cellphones (and the software they contain) are *more* valuable in the market than those that are locked—at least to the device owners.[1050] But the same may not be true with respect to the unlocking of new, carrier-subsidized prepaid cellphones, where it appears that such unlocking may facilitate illicit and commercially harmful activities. For this reason, as discussed below, the Register recommends that any unlocking exemption for cellphones be tailored to exclude unlocking in that context.

With respect to Classes 12 through 14—comprising all-purpose tablet computers, portable mobile connectivity devices, and wearable computing devices—there is no evidence in the record to suggest that unlocking of used devices will cause market harm.

In sum, as a general matter, the Register concludes that the unlocking of used cellphones and other wireless devices as described in Classes 11 through 14 to render them interoperable with alternative networks is likely to be a fair and noninfringing use, except in the case of certain illicit unlocking practices, which accordingly should be excluded from the scope of the exemption.

ii. Proposed Class 15: Consumer Machines

Unlike for the above classes, the record does not establish that the proposed exemption for all "consumer machines" and "smart devices" would facilitate any noninfringing uses. CCA's failure to provide any information about the kinds of devices covered by the proposed exemption makes it impossible to evaluate, among other things, whether unlocking would require creation of copies or derivative works, whether the owners of such devices are likely to own the software that operates those devices, and whether permitting unlocking is likely to adversely impact the market for copyrighted works for purposes of the fair use analysis. Given those deficiencies in the record, the Register cannot conclude that granting an exemption for Proposed Class 15 is likely to facilitate noninfringing uses.

b. Adverse Effects

i. Proposed Class 11: Wireless Telephone Handsets

The Register concludes that there is substantial evidence on this record that consumers are likely to be adversely impacted by an inability to unlock their cellphones. Most significantly, consumers who wish to switch to a new wireless carrier must purchase a new phone that will work on that carrier's network, even if they would prefer to keep their existing phone (with its existing embedded software). This places a burden on consumers' use of their cellphones (and noninfringing uses of the software on those phones). Those burdens are particularly notable today given that, as Congress observed in enacting the Unlocking Act, there has been "a shift away from the earlier practice of

[1050] *Id.* at 17.

consumers essentially disposing of their old cellphones after a few years."[1051] Instead, "consumers now use their cell phones for longer periods of time; reuse their devices upon upgrading by giving their older devices to family members; or sell their used devices in a growing marketplace for used phones and then us[e] the proceeds from the sale to offset the cost of replacement devices."[1052] These legitimate uses are hindered by the ban on circumvention.

The Register likewise concludes that the prohibition on circumvention would likely have an adverse impact on the activities of bulk recyclers, charities, and other entities that purchase used cellphones and unlock them for redistribution or resale. This legitimate activity facilitates a broader market for used cellphones (and the copyrighted software they contain).[1053]

The Register also concludes that the potential available alternatives to circumvention are insufficient to mitigate these adverse effects. First, proponents have put forward unrebutted evidence that consumers may have trouble taking advantage of voluntary carrier unlocking policies because of the conditions imposed by certain wireless carriers.[1054] And it is undisputed that these voluntary carrier policies may not accommodate the needs of legitimate bulk recyclers.[1055] Second, the record reflects that the availability of new, unlocked cellphones in the marketplace does not fully mitigate the adverse effects flowing from the inability to unlock used, locked cellphones.[1056] And third, as CCA explains, consumers with very specific device requirements—such as consumers with disabilities—may not find the precise device they desire as an unlocked option.[1057]

Although Consumers Union and eBay/Gazelle ask that the exemption be extended to new phones and tablets still under contract, they have failed to put forward convincing evidence of any cognizable adverse effects stemming from consumers' inability to unlock such cellphones. As explained above, testimony at the public hearing indicated that it was not reasonable to assume that this would be a realistic possibility when purchasing a subsidized device, as the seller would presumably require such a device to be activated by the purchaser.

[1051] H.R. REP. NO. 113-356, at 3.

[1052] *Id.*

[1053] *See* 2010 Final Rule, 75 Fed. Reg. at 43,831-32.

[1054] *See* Consumers Union Class 11 Supp. at 18-19; *see also* S. REP. NO. 113-212, at 2 (2014) (observing that there were "circumstances in which additional avenues for unlocking may be preferable over attempting to unlock through the carrier").

[1055] ISRI Class 11 Supp. at 18.

[1056] *Id.* at 20. By contrast, in the 2012 proceeding, proponents failed to make any meaningful showing in this regard. 2012 Recommendation at 95-96.

[1057] CCA Class 11 Supp. at 9.

ii. Proposed Class 12: All-Purpose Tablets

As noted, the key issue concerning the unlocking of all-purpose tablets is the extent to which tablet devices are locked to a particular wireless carrier. Although it appears that most tablets with mobile data connections are not locked at the time of purchase, the evidence shows that at least some tablets are sold with carrier locks.[1058] The evidence of the adverse effects that flow from that fact is essentially the same as that addressed above for cellphones: the ban on circumvention burdens consumers' ability to switch wireless carriers, and impedes legitimate bulk recycling activities. Moreover, the record supports the conclusion that the alternatives to circumvention are inadequate for the same reasons as discussed under Class 11.

iii. Proposed Class 13: Mobile Connectivity Devices

With respect to mobile connectivity devices such as mobile hotspots and removable wireless broadband modems, as mentioned above, it is apparent from the record that at least some such devices are sold locked to a wireless network.[1059] No commenter disputed proponents' claims that the inability to unlock these devices adversely affects users' ability to connect these devices to an alternative wireless carrier's network, or the assertion that carriers' voluntary unlocking policies do not necessarily encompass mobile connectivity devices.[1060]

iv. Proposed Class 14: Wearable Computing Devices

As noted, the central issue in relation to wearable computing devices is the extent to which such devices include mobile data (*e.g.*, 3G/4G) connections, rather than Wi-Fi or Bluetooth connections, and if so, whether they are locked to a particular wireless carrier. Here the evidence was limited: the record put forth by proponents revealed a single smartwatch—the Samsung Gear S—that has a dedicated 3G connection and is sold locked to a wireless carrier.[1061] Proponents assert that more wearable computing devices with mobile data connections are soon likely to be introduced in the marketplace, and that some of these will be locked by wireless carriers. Notwithstanding the very limited selection of consumer wearable devices with mobile data connections currently in the

---

[1058] *See* Consumers Union Class 12 Supp. at Exhibit G (unlocking policy for Sprint) ("Many Sprint phones or tablets . . . have been programmed with a master subsidy lock . . . that locks the device . . . .); *id.* at Exhibit H (unlocking policy for AT&T covering both wireless phones and tablets).

[1059] CCA Class 13 Supp. at 7 (citing AT&T's locking policy, which explicitly states that it places software locks on mobile hotspots it sells).

[1060] *Id.*

[1061] CCA Class 14 Supp. at 4; Tr. at 16:24-17:02 (May 21, 2015); *see also Samsung Gear S-Black* (offering the Samsung Gear S for $99.99 with a two year contract, and $299.99 without a contract). The Register observes that a fitness device was introduced last year that includes a dedicated connection to AT&T's network, although it is not clear whether the device is locked to that network, and proponents have not relied on it. *See Ironman One GPS+*, TIMEX, http://www.timex.com/one-gps (last visited Oct. 7, 2015) (noting that three years of AT&T mobile data service are included).

marketplace, the Register concludes that there is sufficient evidence to support a conclusion that adverse effects are likely to increase in the next three years. In this context, it is appropriate to consider the rapid pace of technological development, especially in the mobile computing context. CCA argues, and no opponent disputes, that batteries and radio transmitters are becoming smaller and smaller, thus making it likely that manufacturers will add dedicated connections to a broader range of wearable devices. And given that wireless carriers have locked other new wireless devices that have been recently introduced, it is reasonable to assume that the same will be true for at least some of the devices introduced in the future.

To the extent such devices are locked to a wireless carrier, the adverse effects flowing from the inability to unlock the devices are the same as for the other classes of devices addressed above. And, as CCA's unrebutted evidence indicates, the carriers' voluntary unlocking policies do not necessarily include wearable devices.[1062]

v. Proposed Class 15: Consumer Machines

As discussed, CCA, the main proponent of the proposed exemption for all "consumer machines," failed to provide any specific information about the kinds of devices that its proposal would encompass. As a result, it is impossible on this record to assess the adverse effects of the ban on circumvention with respect to the devices that might theoretically fall within this proposed class.

c. Statutory Factors

i. Proposed Classes 11 to 14

With respect to the devices covered by Classes 11 to 14 (cellphones, all-purpose tablet computers, mobile connectivity devices, and wearable computing devices), the statutory factors favor an exemption.

The first factor, the availability for use of copyrighted works, favors an exemption. Proponents have provided evidence that unlocking a device can extend its useful life (and, thus, the useful life of the software it contains), because it can be ported to a new wireless carrier. Moreover, devices (and their resident software) can be recycled and made available for use by others. At the same time, there is no evidence in the record to suggest that granting an exemption would discourage the development and dissemination of new wireless device software; to the contrary, experience with the cellphone unlocking exemption suggests that an unlocking exemption has no such adverse effect.

The second factor, the availability for use of works for nonprofit archival, preservation, and educational purposes, and the third factor, the effect on criticism, comment, news reporting, teaching, scholarship and research, are neutral. Although the

[1062] CCA Class 14 Supp. at 8.

Register agrees with proponents that wireless devices are useful tools for education and news consumption, such general observations have little direct connection to the proposed exemption, which is focused on allowing the device to be used on the network of a different wireless carrier.

With respect to the fourth factor, except in the case of prepaid, subsidized cellphones—a matter that can be addressed by an appropriately crafted exemption—the record here supports a finding that the market for wireless device software is unlikely to be affected by enabling consumers to alter that software to connect the device to an alternative network.[1063] Indeed, the record indicates that, during the time that the exemption for cellphone unlocking has been in place, the market for cellphones (including their embedded software) has continued to expand rapidly.[1064] Further, there is nothing in the record to suggest that a different result would obtain for any of the other classes of device.

With respect to the fifth factor, allowing consideration of such factors as the Librarian considers appropriate, the Register agrees with proponents that permitting an exemption is likely to have beneficial effects on consumer choice and competition.

ii. Proposed Class 15: Consumer Machines

As discussed, CCA, the main proponent of the proposed exemption for all "consumer machines," failed to provide any specific information about the kinds of devices that its proposal would encompass. Therefore, it is impossible to analyze the statutory factors with respect to this proposed class.

4. NTIA Comments

According to NTIA, "[p]roponents have offered detailed evidence as to the need for an unlocking exemption, as well as its noninfringing nature."[1065] NTIA urges that the exemption should simply extend to all "used wireless devices," rather than enumerating the types of devices to which the exemption applies.[1066] NTIA asserts that "[t]he record and evidence presented during the hearings demonstrate that, at a software level, there is often little technical difference between these types of devices, and the works at issue are frequently similar or even identical."[1067] NTIA expresses concern that "enumerating a list of covered devices . . . will inevitably prove ambiguous or obsolete within the next three years."[1068]

[1063] *See* 2012 Recommendation at 98 (reaching same conclusion with respect to cellphones).

[1064] *See, e.g.*, CCA Class 11 Supp. at 12.

[1065] NTIA Letter at 39.

[1066] *Id.* at 42.

[1067] *Id.*

[1068] *Id.*

NTIA acknowledges the record shows a "lack of desire" on the part of consumers to unlock wireless hotspots embedded in motorized vehicles, and notes that such unlocking "is not achievable without destroying the vehicle."[1069] Accordingly, NTIA states that it "would not oppose the exclusion of wireless [devices] embedded in vehicles from the exemption at this time."[1070]

The Register concludes based on the record that the exemption should set forth, at least in general terms, the types of devices to which it applies. This approach is consistent with Congress's intent that exemptions be focused and reflect marketplace developments. Such an approach is also more consistent with the record in this proceeding. Notably, proponents have excluded one type of wireless device—vehicle-based hotspots—from their request, and NTIA does not oppose this exclusion. Moreover, there was no evidence offered to explain the potentially expansive class of "consumer machines" that would be covered by the exemption. In any event, notwithstanding the specification of categories, as discussed below, the Register has recommended granting exemptions for a broad range of devices.

5. Conclusion and Recommendation

Proponents of Classes 11 to 14 have demonstrated that in the absence of an exemption to allow circumvention, owners of cellphones, all-purpose computing tablets, mobile connectivity devices, and wearable computing devices will be adversely affected in their ability to unlock those devices to connect to a different wireless carrier. This includes entities that obtain used cellphones and unlock them in bulk for redistribution or resale. In addition, three of the five statutory factors tend to favor the proponents, while the other two are neutral. The Register therefore recommends that exemptions for these classes be granted, although some points of clarification are in order.

First, unlike past rulemakings where the finding of noninfringing use rested solely on section 117, the Register here also concludes that the exemption is likely to facilitate fair use of the computer programs on the covered devices. Because, unlike the section 117 privilege, fair use is not limited to the owner of the computer program, there is no need for the Register to limit the exemption to such persons. Moreover, because the Unlocking Act[1071] and the resulting rule[1072] already specify the persons who are entitled to initiate circumvention, there is no need for the exemption to do the same.

Second, there was universal agreement that any exemption for cellphones should be fashioned so as to exclude trafficking activities that seek illegitimately to profit from subsidies offered by prepaid phone providers. As in previous proceedings, the Register concludes that the requirement that the wireless devices be "used" should be adequate to

[1069] *Id.*

[1070] *Id.*

[1071] Unlocking Act § 2(c).

[1072] *See* 37 C.F.R. § 201.40(c).

exclude such trafficking from the reach of the exemption.[1073] The Register, however, adopts ISRI's proposal to clarify that a device is "used" if it "has been lawfully acquired and activated on the wireless telecommunications network of a carrier."[1074]

The Register has considered TracFone's request for an exemption that adds additional conditions (such as requiring that all legal obligations to the original wireless carrier be satisfied before the device is unlocked). The Register has concluded, however, that adopting these conditions would render the exemption unwieldy in practice. For instance, ISRI notes that it would be difficult for downstream purchasers of locked cellphones to assess whether legal obligations to the original wireless carrier were satisfied.[1075] In any event, TracFone suggested that its concerns could be alleviated through "official comments in the record making clear that the intent of the exemption is not to benefit traffickers," a caveat that is emphasized above.[1076]

Third, the exemption for mobile connectivity devices should be clarified to confirm that it is limited to devices such as those specified in the NPRM, *e.g.*, hotspots and removable wireless broadband modems. The Register understands that proponents do not seek to circumvent wireless connectivity devices that are embedded in "mobile" motor vehicles, such as in-vehicle telematics and communications systems, for unlocking purposes, and that in any event it does not appear to be feasible to do so. Based on this, the Register recommends devices embedded in motor vehicles be excluded from the exemption by including the condition that the devices be "portable."

In contrast to Classes 11 through 14, as the above discussion indicates, proponents of Class 15, encompassing a broad and undefined range of "consumer machines" or "smart devices," have failed to make a case for an exemption. Proponents declined to provide any specific information about the kinds of devices the proposal encompasses, what noninfringing uses would be facilitated by circumvention of TPMs on those devices, or any adverse effects understood to flow from the prohibition on circumvention. The Register therefore recommends that the proposed exemption in Class 15 be denied.

Accordingly, the Register recommends that the Librarian designate the following classes:

> **(i) Computer programs that enable the following types of wireless devices to connect to a wireless telecommunications network, when circumvention is undertaken solely in order to connect to a wireless telecommunications network and such connection is authorized by the operator of such network, and the device is a used device:**

[1073] 2010 Recommendation at 169.

[1074] *See, e.g.*, ISRI Class 11 Supp. at 14.

[1075] ISRI Class 11 Reply at 8-9.

[1076] TracFone Opp'n at 7.

(A) Wireless telephone handsets (*i.e.*, cellphones);

(B) All-purpose tablet computers;

(C) Portable mobile connectivity devices, such as mobile hotspots, removable wireless broadband modems, and similar devices; and

(D) Wearable wireless devices designed to be worn on the body, such as smartwatches or fitness devices.

(ii) A device is considered "used" for purposes of this exemption when it has previously been lawfully acquired and activated on the wireless telecommunications network of a wireless carrier.

E. Proposed Classes 16 and 17: Jailbreaking – Smartphones and All-Purpose Mobile Computing Devices

Proposed Classes 16 to 20 each address an activity commonly known as "jailbreaking." As the Register has previously explained, "jailbreaking" refers to the process of gaining access to the operating system of a computing device, such as a smartphone or tablet, to install and execute software that could not otherwise be installed or run on that device, or to remove pre-installed software that could not otherwise be uninstalled.[1077] Each proposal in Classes 16 through 20 covers a different type of device. This section addresses Proposed Classes 16 and 17, directed to smartphones and all-purpose mobile computing devices (including tablets) respectively; the remaining classes are each considered in their own sections below.

1. Proposals

EFF filed a petition seeking a jailbreaking exemption for all "mobile computing devices," including wireless telephone handsets that are capable of running a wide range of applications (*i.e.*, "smartphones") and tablet computers ("tablets").[1078] EFF explains that "[m]obile device users jailbreak for a variety of reasons, such as to install the latest fixes for security vulnerabilities, to keep the software on a device current after the manufacturer has stopped supporting it, and to run many kinds of important and useful software excluded by the manufacturer."[1079] EFF's petition specifies that the requested exemption is "not intended to apply to computer programs running on devices designed primarily for the consumption of a single type of media, such as dedicated e-book readers, nor to programs running on desktop or laptop computers."[1080] In addition to EFF's proposal, Maneesh Pangasa filed a separate petition seeking an exemption for tablet computers.[1081]

[1077] 2012 Recommendation at 66 & n.306; *see also* Electronic Frontier Foundation ("EFF") Class 16 Supp. at 6-7 (describing process of jailbreaking); Jay Freeman Class 16 Supp. at 4-5 (same). According to EFF, the act of gaining administrative access to a device's operating system is variously referred to as "jailbreaking," "rooting," or "unlocking a bootloader" depending upon the mobile device platform, although the terms are sometimes used interchangeably. EFF Class 16 Supp. at App. A (Statement of Dr. Jeremy Gillula at 1-2). For ease of reference, all such processes will be referred to here as "jailbreaking." A smartphone's operating system can also be referred to as "firmware." *See id.* at 4 n.16. Although the terms "firmware" and "software" are variously used throughout the Recommendation, both are considered computer programs within the meaning of the Copyright Act. *See* 17 U.S.C. § 101 (definition of "computer program").

[1078] EFF's proposed exemption encompassed "[c]omputer programs that enable mobile computing devices, such as telephone handsets and tablets, to execute lawfully obtained software, where circumvention is accomplished for the sole purposes of enabling interoperability of such software with computer programs on the device, or removing software from the device." EFF Jailbreaking Pet. at 1.

[1079] *Id.* at 2.

[1080] *Id.*

[1081] Pangasa's tablet jailbreaking petition encompassed two distinct proposals, one for all-purpose tablets and one for e-book readers. Pangasa Tablet and E-Book Reader Jailbreaking Pet. at 1-4. The Office

The Copyright Office divided these proposals into two proposed classes to ensure an adequate administrative record on which to make a recommendation.[1082] The first encompasses smartphones,[1083] and was described in the NPRM as follows:

> Proposed Class 16: This proposed class would permit the jailbreaking of wireless telephone handsets to allow the devices to run lawfully acquired software that is otherwise prevented from running, or to remove unwanted preinstalled software from the device.[1084]

Along with EFF, comments supporting Proposed Class 16 were filed by New Media Rights ("NMR"),[1085] Free Software Foundation ("FSF"),[1086] Catherine Gellis and the Digital Age Defense project ("Gellis/Digital Age Defense"),[1087] and Jay Freeman, the proprietor of an app store for jailbroken devices.[1088] In addition, over 2000 individuals filed comments in support of Proposed Class 16.[1089]

The other class encompasses "all-purpose mobile computing devices," including tablets, and was described in the NPRM as follows:

> Proposed Class 17: This proposed class would permit the jailbreaking of all-purpose mobile computing devices to allow the devices to run lawfully acquired software that is otherwise prevented from running, or to remove unwanted preinstalled software from the device. The category "all-

---

consolidated the portion of Pangasa's petition addressing jailbreaking of general-purpose tablets with EFF's proposal in Proposed Class 17. *See id.* at 1 ("I would like to request an exemption to the Digital Millennium Copyright Act for jail-breaking or rooting tablets like the Apple iPad Air & iPad Mini, Amazon's Kindle Fire HD, Microsoft Surface line of tablets (particularly the RT version to install hacks that permit running desktop applications on RT devices)."). Pangasa's proposal with respect to e-book readers is addressed in Proposed Class 18.

[1082] In 2012, based on the Register's Recommendation, the Librarian granted a jailbreaking exemption for smartphones, but not for tablets, on the ground that there was an insufficient record to develop "an appropriate definition for the 'tablet' category of devices." 2012 Final Rule, 77 Fed. Reg. at 65,264.

[1083] The Register uses the term "smartphone" in Class 16 to refer specifically to those wireless telephone handsets that are capable of running a wide variety of software applications. In contrast, in the unlocking exemption in Class 11, the Register uses the more general terms "cellphones" or "wireless telephone handsets," because the unlocking exemption is potentially relevant to all types of mobile phones, not just smartphones.

[1084] NPRM, 79 Fed. Reg. at 73,866-67.

[1085] NMR Class 16 Supp.

[1086] FSF Class 16 Supp.

[1087] Gellis/Digital Age Defense Class 16 Supp.

[1088] Freeman Class 16 Supp.

[1089] *See* Digital Right to Repair Class 16 Supp. (2087 individuals); AK Wong Class 16 Supp.; Andrew de Kroon Class 16 Supp.; Anthony Marquez Supp.; Blinky X Supp.; David Darling Supp.; Edward Winget Jr. Supp.; Eli Cantarero Supp.; Jeffrey Philip Roddy Supp.; Kevin Chen Class 16 Reply; Kyle Moschell Class 16 Supp.; Micah Ross Supp.; Nathan Vahrenberg Supp.; Robert Ross Class 16 Supp.

> purpose mobile computing device'' includes all-purpose non-phone devices (such as the Apple iPod touch) and all-purpose tablets (such as the Apple iPad or the Google Nexus). The category does not include specialized devices such as e-book readers or handheld gaming devices, or laptop or desktop computers.[1090]

In addition to EFF, comments supporting Proposed Class 17 were filed by NMR,[1091] FSF,[1092] Gellis/Digital Age Defense,[1093] Freeman,[1094] and nearly 1900 individuals.[1095]

Because the proposed exemptions for jailbreaking of smartphones and all-purpose mobile computing devices involve overlapping factual and legal issues, Proposed Classes 16 and 17 are discussed together.

a. Background

According to EFF, "controls within the firmware on nearly all phones (and other mobile devices)," including all-purpose tablets and handheld computing devices such as the iPod touch, "prevent the owner of the device from installing, removing or modifying software to some degree."[1096] EFF notes that either Apple's iOS or Google's Android operating system is installed on the vast majority of smartphones and all-purpose tablets and that both operating systems use access controls.[1097]

EFF explains that iOS "contains cryptographic verification that prevents any application from running on a device unless it bears a digital signature from Apple."[1098] In addition, iOS "contains cryptographic checks at various levels of the software stack that prevent modification or replacement of the operating system itself."[1099] On Android devices, the "fundamental access control . . . is the bootloader," which "verifies the

[1090] NPRM, 79 Fed. Reg. at 73,867.

[1091] NMR Class 17 Supp.

[1092] FSF Class 17 Supp.

[1093] Gellis/Digital Age Defense Class 17 Supp.

[1094] Freeman Class 17 Supp.

[1095] *See* Digital Right to Repair Class 17 Supp. (1884 individuals); Andrew de Kroon Class 17 Supp.; Christian Clark Class 17 Reply; David Garver Supp.; Evan Abitbol Reply; George G. Deriso Supp.; Juan Pablo Zapata Díaz Class 17 Reply; Kyle Moschell Class 17 Supp.; Michael Horton Class 17 Reply; Nathan Scandella Supp.; Robert Ross Class 17 Supp. Petitioner Pangasa did not file written comments in support of his proposal.

[1096] EFF Class 16 Supp. at 4; EFF Class 17 Supp. at 5 (same).

[1097] EFF states that as of October 2014, iOS and Android together "control 94.2% of smartphones." EFF Class 16 Supp. at 4. And, according to EFF, worldwide in 2014, "iPads (running iOS) represented about 27% of tablet sales, whereas tablets running Android made up about 67% of the market." EFF Class 17 Supp. at 5.

[1098] EFF Class 16 Supp. at 4; *see also* EFF Class 17 Supp. at 5.

[1099] EFF Class 16 Supp. at 4; *see also* EFF Class 17 Supp. at 5-6.

operating system on the device cryptographically, and will refuse to run an operating system not approved by the device manufacturer, or one that has been modified."[1100] The Android operating system, in turn, "does not allow the device owner, or any programs installed by the owner, to acquire full administrative access to the device," which limits the functionality and data that the user or application can access.[1101] The Android operating system also "prohibits the user from *removing* unwanted programs that were installed by the manufacturer."[1102] EFF also explains that other, less-common mobile operating systems, such as Windows Phone and BlackBerry OS, contain similar access controls.[1103]

According to EFF, "[j]ailbreaking most mobile devices requires making use of a security vulnerability in either the operating system or the bootloader."[1104] On iOS devices, jailbreaking involves "modifying the firmware so that it will run software code without checking to see if the code has been cryptographically signed by Apple."[1105] On Android devices, jailbreaking involves modifying the bootloader to permit loading of a modified operating system.[1106]

The Register has twice before recommended, and the Librarian has twice adopted, an exemption permitting jailbreaking of smartphones.[1107] The current smartphone exemption covers:

> [c]omputer 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.[1108]

In previously recommending adoption of this exemption, the Register concluded that the intended use—to render certain lawfully acquired applications interoperable with the handset's software—was likely fair.[1109] Further, the Register concluded that consumers were adversely impacted by TPMs preventing jailbreaking, and that this impact was not

[1100] EFF Class 16 Supp. at 5; *see also* EFF Class 17 Supp. at 6.

[1101] *Id.*

[1102] EFF Class 16 Supp. at 5; *see also* EFF Class 17 Supp. at 6-7.

[1103] EFF Class 16 Supp. at 6; EFF Class 17 Supp. at 7 (emphasis in original).

[1104] EFF Class 16 Supp. at 7; *see also* Freeman Class 17 Supp. at 6 (explaining that access controls can be circumvented by exploiting "common software security vulnerabilities such as 'buffer overruns,' 'use-after-frees' and 'format string attacks'").

[1105] EFF Class 17 Supp. at 7.

[1106] *See id.*; *see also* EFF Class 16 Supp. at App. A (Statement of Dr. Jeremy Gillula at 2) (describing process of jailbreaking an Android device running version 2.3 of the operating system).

[1107] 2010 Final Rule, 75 Fed. Reg. at 43,830-32; 2012 Final Rule, 77 Fed. Reg. at 65,263-66.

[1108] 2012 Final Rule, 77 Fed. Reg. at 65,263.

[1109] 2012 Recommendation at 74; *see also* 2010 Recommendation at 100.

mitigated by available alternatives to circumvention.[1110] Proponents seek not only to continue the jailbreaking exemption for smartphones but also to expand it to specifically permit removal of unwanted preinstalled software.[1111]

In the 2012 rulemaking, the Register also considered for the first time a proposed exemption permitting jailbreaking of "tablet" computers. The Register recommended against adopting that exemption on the ground that there was an insufficient record to develop "an appropriate definition for the 'tablet' category of devices."[1112] In the current rulemaking, as noted above, proponents renew the request for an exemption to cover general-purpose mobile computing devices, including tablets. In response to opponents' concerns, described below, about the uncertain scope of the proposed exemption, EFF offered two further criteria to define such devices: first, that they are portable, in the sense that they are "designed to be carried or worn;" and second, that they "come equipped with an operating system that is primarily designed for mobile use," such as Android, iOS, Blackberry OS, and Windows Phone.[1113] This additional limitation would exclude devices that run operating systems designed for desktops or laptops, such as Mac OS and Windows 8.[1114]

In arguing for the exemption in Proposed Class 17, proponents urge the Office to avoid distinguishing between smartphones and all-purpose mobile computing devices, such as tablets and handheld computers, for purposes of the jailbreaking exemptions. According to EFF, "[t]hough mobile computing devices can be subdivided based on their size and their ability to make and receive telephone calls, they are in many respects a single category of device."[1115] EFF notes that "[t]he same mobile firmware, primarily Apple's iOS and varieties of the Android operating system, is sold on smartphones, tablets, and other handheld devices such as the iPod Touch."[1116] Indeed, according to Freeman, "[t]he iPhone, iPad, iPod touch, and Apple TV . . . all run the *exact same* code from Apple for their operating system," and "Samsung's Galaxy S5 (a phone), Galaxy Tab (a tablet), and their 'Smart TV' all use *virtually identical code* from Google for their operating system."[1117] Additionally, EFF asserts that "smartphones and tablets are largely able to run the same applications," and that "[t]he common practice among software

[1110] 2012 Recommendation at 76; *see also* 2010 Recommendation at 100.

[1111] EFF Jailbreaking Pet. at 2.

[1112] 2012 Final Rule, 77 Fed. Reg. at 65,264.

[1113] Tr. at 50:12-20 (May 21, 2015) (Stoltz, EFF).

[1114] EFF Class 17 Supp. at 3-4.

[1115] *Id.* at 2; *see also* Tr. at 58:09-25, Exhibit 8 (May 21, 2015) (Charlesworth, USCO; Freeman, SaurikIT) (photographs of devices showing differences in size).

[1116] EFF Class 17 Supp. at 2.

[1117] Freeman Class 17 Supp. at 2 (emphasis in original). Although Freeman mentioned the Apple TV, at the public hearing on Proposed Classes 16 and 17, he confirmed that he was not seeking an exemption permitting jailbreaking of a dedicated media consumption device like the Apple TV. Tr. at 56:03-16 (May 21, 2015) (Freeman, SaurikIT).

developers is to write software that is meant to be used on both phones and tablets."[1118] And, according to EFF, "[m]ost phones and tablets use the same processor architecture, known as ARM, giving a degree of uniformity to the development process across devices."[1119]

EFF also claims that even "the presence or absence of particular types of cellular radio hardware" does not always "distinguish phones from tablets."[1120] EFF notes that the 4G LTE cellular communications protocol "treats voice calls and data transmissions identically, meaning that any phone or tablet that uses LTE can make and receive voicecalls . . . regardless of whether the device is marketed as a phone."[1121] EFF also notes that the growing market for "phablets," which are "devices of intermediate size between a smartphone and a tablet and that function as either," demonstrates the difficulty of drawing meaningful distinctions between different categories of general-purpose mobile devices.[1122] EFF thus concludes that "[s]martphones and tablets today are best seen as a continuum of devices varying primarily by size, rather than distinct categories."[1123]

At the same time, EFF believes it is appropriate to distinguish mobile computing devices from laptop and desktop PCs, noting that there are technical differences between those platforms and that "PC operating systems do not, as yet, impose the sort of severe restrictions on which applications can be run, and what those applications can do, which are the norm for mobile devices."[1124] EFF also believes it appropriate to distinguish between mobile computing devices and "dedicated media consumption devices such as e-book readers and handheld gaming devices," as those devices "do not come with general-purpose operating systems capable of running a large variety of application software."[1125] Thus, as EFF explains, while the Kindle Paperwhite, as a dedicated e-book reader, would not fall within the scope of the requested exemption, the Kindle Fire, as a general-purpose mobile computing device, would.[1126]

[1118] EFF Class 17 Supp. at 2; *see also* Freeman Class 17 Supp. at 2 ("[I]t is one of the primary benefits of these platforms . . . that all different devices can easily be targeted by developers using a single development toolchain [so that] a single resulting 'app' not only can be but *should* be usable on all classes of device.") (emphasis in original).

[1119] EFF Class 17 Supp. at 2-3.

[1120] *Id.* at 3.

[1121] *Id.*

[1122] *Id.*

[1123] *Id.*

[1124] *Id.* at 3-4.

[1125] *Id.* at 4.

[1126] *Id.* Proponent Freeman appeared to disagree with EFF to some extent on this point; as discussed in Proposed Class 18, Freeman asserts that "[a]n e-book reader that is 'only' an e-book reader . . . up until the moment that someone jailbreaks it: then it becomes like any other device." Freeman Class 18 Supp. at 3.

b. Asserted Noninfringing Uses

Proponents make virtually identical arguments to support the claims that jailbreaking of smartphones and all-purpose mobile computing devices constitute fair uses of mobile computing device software under section 107.[1127] Relying on case law and determinations of the Register in earlier section 1201 rulemakings, EFF maintains that "modifying the firmware in one's device in order to run lawfully acquired software . . . fall[s] squarely within Congress's intent to promote software interoperability."[1128] EFF explains that the Register found smartphone jailbreaking to be a fair use in the 2012 and 2010 proceedings[1129] and that BSA | The Software Alliance ("BSA"), the sole opponent of the exemption, does not dispute the noninfringing nature of jailbreaking in its comments.[1130]

According to EFF, the purpose and character of jailbreaking "weighs heavily in favor of a finding of fair use."[1131] EFF relies in particular on the Ninth Circuit's decisions in *Sega Enterprises Ltd. v. Accolade, Inc.* and *Sony Computer Entertainment, Inc. v. Connectix Corp.*, which concluded that reverse-engineering video game systems in order to facilitate the creation of interoperable third-party software is a fair use.[1132] EFF argues that the copying in *Sega* and *Connectix* is analogous to jailbreaking because it also enables "greater access to information" and facilitates the creation of new, independent software that can run on the device.[1133] EFF points as well to the Register's findings in 2010 and 2012 that Congress affirmed the holdings of *Sega* and *Connectix* in the legislative history of section 1201, "express[ing] a commitment to permit and encourage interoperability."[1134]

EFF further argues that jailbreaking is noncommercial and transformative under the first fair use factor.[1135] EFF asserts that jailbreaking is transformative because it allows smartphones and mobile devices, and the firmware contained on them, "to be used

---

[1127] *See, e.g.*, EFF Class 16 Supp. at 7-14; EFF Class 17 Supp. at 7-13. Proponents did not rely on section 117 as legal support for Classes 16 or 17. Section 117 permits the owner of a copy of a computer program to reproduce and adapt the program in certain circumstances, and thus potentially could be relevant to jailbreaking activities. *See* 17 U.S.C. § 117. Prior rulemakings, however, have relied on fair use as the basis to find that jailbreaking can facilitate noninfringing uses. 2012 Recommendation at 74; 2010 Recommendation at 92-93.

[1128] EFF Class 16 Supp. at 7; EFF Class 17 Supp. at 9.

[1129] *Id.*

[1130] EFF Class 16 Reply at 3; EFF Class 17 Supp. at 6.

[1131] EFF Class 16 Supp. at 9; EFF Class 17 Supp. at 11.

[1132] EFF Class 16 Supp. at 8 (discussing *Sega*, 977 F.2d 1510, 1514 (9th Cir. 1992), *as amended* (Jan. 6, 1993), and *Connectix*, 203 F.3d 596, 608 (2000)); EFF Class 17 Supp. at 9 (same).

[1133] EFF Class 16 Supp. at 8; EFF Class 17 Supp. at 9.

[1134] EFF Class 16 Supp. at 8 (quoting 2010 Recommendation at 92; 2012 Recommendation at 71-72); EFF Class 17 Supp. at 9-10 (same).

[1135] EFF Class 16 Supp. at 9; EFF Class 17 Supp. at 10-11.

for new purposes, imbuing them with further usefulness, personalization, and meaning."[1136] EFF states that jailbreaking is noncommercial because smartphone and device owners who jailbreak "do not do so for profit, but rather to enhance and personalize their devices,"[1137] and that jailbreaking serves a public purpose by "promot[ing] additional creativity and expand[ing] access to knowledge."[1138]

EFF argues that the second fair use factor, the nature of the copyrighted work, weighs in favor of fair use, because "bootloaders and operating systems are largely functional works."[1139] It asserts that this view is consistent with the Federal Circuit's 2014 decision in *Oracle America, Inc. v. Google Inc.*, in which the court observed that "'where the nature of the work is such that purely functional elements exist in the work and it is necessary to copy the expressive elements in order to perform those functions, consideration of this second factor arguably supports a finding that the use is fair.'"[1140] EFF further argues that because access controls on smartphones and mobile devices "are dictated almost entirely by external considerations" and "*must* be used to enable compatibility with independently created programs," the second factor tilts in favor of fair use.[1141]

With respect to the third fair use factor, the amount and substantiality of the portion of the work used, EFF asserts that the portion used need only be "'reasonable' and for a legitimate purpose."[1142] EFF appears to acknowledge that circumvention may require copying of the device firmware in its entirety, but cites examples from case law where the copying of whole works was deemed to be "necessary to achieving a favored purpose" and therefore fair.[1143] EFF argues that "the amount of code copied in the course of a jailbreak is necessary and reasonable for the purpose of ensuring interoperability with third party applications."[1144] EFF further states that the amount of code that is actually modified is sometimes *de minimis*, thus minimizing the significance of this

[1136] EFF Class 16 Supp. at 9; EFF Class 17 Supp. at 10.

[1137] *Id.*

[1138] *Id.*

[1139] EFF Class 16 Supp. at 10; EFF Class 17 Supp. at 11.

[1140] EFF Class 16 Supp. at 10 (quoting *Oracle v. Google*, 750 F.3d 1339, 1375 (Fed. Cir. 2014)); EFF Class 17 Supp. at 11-12 (same). While the Federal Circuit discussed fair use in *Oracle v. Google*, it ultimately concluded that the factual record on fair use was insufficient and remanded for additional fact finding. *Oracle v. Google*, 750 F.3d at 1377.

[1141] EFF Class 16 Supp. at 10-11; EFF Class 17 Supp. at 12. EFF further argues that device access controls are equivalent to "lockout codes" which are either uncopyrightable, or only bear thin copyright protection. *See* EFF Class 16 Supp. at 11; EFF Class 17 Supp. at 12.

[1142] EFF Class 16 Supp. at 11 (quoting *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 586 (1994)); EFF Class 17 Supp. at 12 (same).

[1143] EFF Class 16 Supp. at 11-12 (citing *Sega*, 977 F.2d at 1526 and *Connectix*, 203 F.3d at 605-06); EFF Class 17 Supp. at 12-13 (same).

[1144] EFF Class 16 Supp. at 12; EFF Class 17 Supp. at 13.

factor in those instances.[1145] EFF therefore asserts that the third factor either favors fair use or is neutral.[1146]

For the fourth factor, EFF asserts that no market harm to the smartphone market has been shown as a result of the grant of the smartphone jailbreaking exemption in the past.[1147] To the contrary, it claims that the evidence indicates continued growth in this market.[1148] EFF notes that "[t]he percentage of U.S. adults who are smartphone users has increased by 23% since 2011 to 58%, but among millennials (people in the 18-34 age group), smartphone ownership is nearly universal at 85%."[1149] EFF urges that the same result would hold true if an exemption were extended to all-purpose mobile devices.[1150] In this regard, EFF notes that "jailbreaking does not foreclose sales of mobile device firmware, nor are users jailbreaking their devices to compete in the marketplace for firmware sales."[1151] Indeed, EFF argues that rather than causing harm, "jailbreaking contributes to the success of" the relevant markets because it "push[es] the entire mobile device industry towards improved performance, security, and functionality."[1152]

Proponents additionally maintain that the marketplace for manufacturer-approved apps has thrived notwithstanding the existing exemption. For instance, Kevin Chen, an iOS app developer, states that "there has been no detrimental effect on the profitability of app developers like me, or on the innovation and variety of apps."[1153] EFF further notes that any harm resulting from other types of legitimate competition—for example, because device owners prefer to install third-party apps—is not cognizable under the fourth factor.[1154] Overall, EFF urges that jailbreaking is a noninfringing fair use.[1155]

c. Asserted Adverse Effects

Proponents again rely on the same asserted adverse effects for both Class 16 and Class 17.[1156] EFF argues that the "exemptions granted by the Librarian in 2010 and 2012 for jailbreaking phones removed a cloud of legal uncertainty from phone owners, and spurred vibrant markets and communities of developers,"[1157] and it asserts that

---

[1145] *Id.*

[1146] *Id.*

[1147] EFF Class 16 Supp. at 12-13; EFF Class 17 Supp. at 13-14.

[1148] EFF Class 16 Supp. at 12; EFF Class 17 Supp. at 14.

[1149] EFF Class 16 Supp. at 2.

[1150] *Id.* at 12-13; EFF Class 17 Supp. at 13-14.

[1151] EFF Class 17 Supp. at 14; *see also* EFF Class 16 Supp. at 12 (same with respect to smartphones).

[1152] EFF Class 16 Supp. at 13; EFF Class 17 Supp. at 14.

[1153] Chen Class 16 Reply at 1-2; *see also* EFF Class 17 Supp. at 19-20.

[1154] EFF Class 16 Supp. at 12; EFF Class 17 Supp. at 14.

[1155] EFF Class 16 Supp. at 13; EFF Class 17 Supp. at 14.

[1156] *See, e.g.*, EFF Class 16 Supp. at 13-21; EFF Class 17 Supp. at 14-19.

[1157] EFF Class 17 Supp. at 14.

"[e]xtending an exemption to mobile devices such as tablets that run the same operating systems as smartphones would extend the benefits of the earlier exemptions."[1158] At the same time, EFF urges that rejecting the exemption for jailbreaking of smartphones "would be a leap backwards for personal data security, mobile innovation, consumer choice and competition."[1159]

Proponents present a series of alleged benefits arising from the ability to jailbreak smartphones and mobile computing devices. EFF observes that independent security researchers can uncover certain vulnerabilities in smartphones and mobile devices only by examining jailbroken devices, pointing to the example of an independently discovered Apple iOS flaw in the Secure Sockets Layer code that provides security for internet traffic but could only be found by jailbreaking an iOS device and accessing its "lower-level functionality."[1160] Proponents point to evidence that security vulnerabilities are often patched through official channels only after several weeks or months, whereas a user can patch her own device immediately if it is jailbroken.[1161] They also note a number of privacy and security-enhancing features that are only available on jailbroken devices, such as the ability to install third-party firewall and permission control apps on jailbroken devices.[1162]

EFF and NMR further explain that smartphone and mobile device manufacturers reject apps from official distribution channels based on private selection criteria and to prevent competition with their own products, thereby stifling the creative expression of users and independent developers.[1163] For example, EFF notes that Apple "has excluded a game with marijuana related content, a game that depicts the ongoing civil war in Syria, an app that reports the locations of U.S. military drone strikes, and a dictionary app (reportedly because it contained objectionable words)."[1164] In addition, "[b]oth Apple and Google reject applications that use payment systems run by other companies for the

[1158] *Id.*

[1159] EFF Class 16 Supp. at 13. No party analyzes the applicability of section 1201(f), which permits certain acts of reverse engineering. But as the Register concluded in 2012, that provision does not authorize the full range of activities requested here. *See* 2012 Recommendation at 85.

[1160] EFF Class 16 Supp. at 13, App. A (Statement of Marc Rogers at 1) (noting that access to lower-level functionality is "necessary to detect many security threats"); EFF Class 17 Supp. at 1 (same). A proposed exemption to permit security research across all devices and software is addressed under Class 25.

[1161] EFF Class 16 Supp. at 13-14; EFF Class 16 Supp. at App. A (Supplemental Material on Jailbreaking at 1-2); EFF Class 16 Supp. at App. A (Statement of Marc Rogers at 2) (describing security vulnerabilities in mobile phones and comparing the effect of such vulnerabilities on jailbroken and non-jailbroken phones); *see also* Freeman Class 16 Supp. at 9; NMR Class 16 Supp. at 23.

[1162] EFF Class 16 Supp. at 15; EFF Class 17 Supp. at 16-17; *see also* Freeman Class 16 Supp. at 9; Freeman Class 17 Supp. at 9; FSF Class 16 Supp. at 1; FSF Class 17 Supp. at 1.

[1163] EFF Class 16 Supp. at 17; EFF Class 17 Supp. at 19; NMR Class 16 Supp. at 20-21; NMR Class 17 Supp. at 20-21.

[1164] EFF Class 16 Supp. at 17; EFF Class 17 Supp. at 19.

purchase of digital goods."[1165] Apple is also said to reject "competing Web browsers, cloud storage services, app choosers, and home screen alternatives" from its app store.[1166]

Proponents also assert that jailbreaking fosters creativity and competition. EFF points in particular to the popularity of Cydia, an online marketplace for non-Apple-approved iOS apps. It notes that, from 2012 to 2014, "between 11.9 million and 16.3 million iOS devices in the U.S. were registered with Cydia."[1167] Freeman, Cydia's proprietor, estimated that "Cydia has been used, at least once, on over 10% of all devices that have ever been sold by Apple."[1168] Freeman also notes that, over six years, Cydia has brought in "$40 million in revenue, with approximately 80% (>$30m) of this having been paid out to developers and artists."[1169] Proponents also note that jailbroken devices are platforms for innovation, explaining that many independent innovations are subsequently incorporated into manufacturers' official releases—such as "[a] rotary lock screen with the ability to unlock and immediately launch specific apps," and "[t]he ability to dismiss individual notifications from the notification area by swiping them," both of which were created by developers for jailbroken smartphones and later incorporated into official Android releases.[1170]

Proponents note other beneficial uses facilitated by jailbreaking as well, including accessibility features for the disabled.[1171] For instance, iOS includes a "Screen Curtain" accessibility feature, which turns off the screen of devices for users who are blind or visually impaired so that they save battery power, but does not provide an easy way for a user to know if that feature is active. To solve this deficiency, a developer created a program called "curtainChecker" for jailbroken iOS devices to audibly inform users if the Screen Curtain feature is active.[1172] In addition, proponents point to the fact that consumers are adversely impacted by loss of performance and storage space resulting

[1165] *Id.*

[1166] *Id.*

[1167] EFF Class 16 Supp. at 6-7; EFF Class 17 Supp. at 8.

[1168] Freeman Class 16 Supp. at 1; Freeman Class 17 Supp. at 1.

[1169] *Id.*

[1170] EFF Class 16 Supp. at 18; EFF Class 17 Supp. at 20; EFF Class 16 Supp. at App. A (Supplemental Material on Jailbreaking at 1) (listing independently developed programs which were later incorporated into official Android releases); *see also* EFF Class 16 Supp. at App. A (Statement of James Wilcox at 1-2) (describing independent software development that requires root access for bug detection and product testing); Freeman Class 16 Supp. at 8; NMR Class 16 Supp. at 18-20.

[1171] *See* Digital Right to Repair Class 17 Supp. at 15 (Abraham Levine) ("My autistic brother's iPad has Springtomize to make the icons large and to make his device easier to use."); Digital Right to Repair Class 17 Supp. at 240 (Brandon Isralsky) ("If you don't let people with disabilities customize their devices, they may not be able to use them."); *see also* Freeman Class 17 Supp. at 7-8; Freeman Class 16 Supp. at 7-8; Blinky X Supp. at 1; Cantarero Supp. at 1-2.

[1172] Freeman Class 16 Supp. at 8; Freeman Class 17 Supp. at 8.

from unwanted software that cannot be removed without jailbreaking the device.[1173] For example, EFF notes that on a Verizon Droid 4 the following apps come preinstalled and cannot be removed without jailbreaking the device: Facebook, Google+, NFL Mobile, Slacker Radio, Amazon Kindle, and Forest Wallpaper.[1174] EFF further observes that jailbreaking reduces consumer electronics waste since it prolongs the lifespan of device hardware by allowing the user to install otherwise unsupported upgrades.[1175] For instance, EFF notes that the Samsung Galaxy Tab was released in September 2010, and that the manufacturer stopped providing updates to the operating system in December 2010; but by jailbreaking the device, more recent versions of the operating system can be installed.[1176] EFF notes that the inability to install software updates can affect the security of the device, because those updates often fix later-discovered security vulnerabilities.[1177]

Proponents and other supporters also argue that market alternatives to jailbreaking do not negate the need for a jailbreaking exemption. First, while acknowledging that "Android devices, whether jailbroken or not, have long given users the ability to load application software from any source,"[1178] EFF and others assert that jailbreaking of Android devices is necessary for other uses covered by the exemption, including removal of unwanted software and installation of security fixes and alternative operating systems.[1179] For instance, EFF explains that "[w]ithout jailbreaking, Android will not run

[1173] EFF Class 16 Supp. at 16 (describing "bloatware" commonly installed on smartphones); EFF Class 17 Supp. at 18 (noting that "[t]ablets and other devices are sold with similar pre-installed software"); EFF Class 16 Supp. at App. A (Supplemental Material on Jailbreaking at 3) (listing software which cannot be removed from an example smartphone); EFF Class 16 Supp. Multimedia Submission (showing software that cannot be removed without jailbreaking).

[1174] EFF Class 16 Supp. at App. A (Supplemental Material on Jailbreaking at 3); EFF Class 17 Supp. at App. A (Supplemental Material on Jailbreaking at 3).

[1175] EFF Class 16 Supp. at 19, App. A (Supplemental Material on Jailbreaking at 2-3) (comparing firmware releases available on jailbroken versus non-jailbroken smartphones); EFF Class 17 Supp. at App. A (Supplemental Material on Jailbreaking at 2-3) (same); *see also, e.g.*, Digital Right to Repair Class 16 Supp. at 202 (individual commenter explaining that although his smartphone was no longer supported by the manufacturer, he was able to continue using the smartphone by jailbreaking it and installing an updated operating system).

[1176] EFF Class 16 Supp. at App. A (Supplemental Material on Jailbreaking at 3); EFF Class 17 Supp. at App. A (Supplemental Material on Jailbreaking at 3).

[1177] EFF Class 16 Supp. at App. A (Supplemental Material on Jailbreaking at 1) (providing examples of "security vulnerabilities that affect older versions of Android and have been fixed in subsequent releases" and noting that "[s]ome devices retain these vulnerabilities because the manufacturer and carriers have ceased to send updates"); EFF Class 17 Supp. at App. A (Supplemental Material on Jailbreaking at 1) (same).

[1178] EFF Class 16 Supp. at 20; EFF Class 17 Supp. at 22.

[1179] *See* EFF Class 16 Supp. at App. A (Supplemental Material on Jailbreaking at 1-2) (providing examples of security defects that can be corrected and new operating systems that can be installed only on jailbroken Android smartphones); EFF Class 17 Supp. at App. A (Supplemental Material on Jailbreaking at 1-2) (same); EFF Class 16 Reply at 3; Freeman Class 16 Reply at 1.

software that requires access to lower-level functionality on the phone."[1180] EFF acknowledges that two manufacturers, Nexus and HTC, have begun to provide an authorized means of jailbreaking certain smartphones.[1181] Nonetheless, it argues that "this development does not eliminate the adverse effects of the ban on circumvention"[1182] in light of the expense of acquiring new smartphone hardware.[1183] Proponents emphasize the small portion of the market currently served by these alternate options; for instance, Freeman noted that "fewer than 1% of users" own a Nexus device.[1184] EFF stresses that "[o]f the hundreds of millions of smartphones in use in the U.S., including Android phones, the overwhelming majority require jailbreaking" in order to engage in the proposed uses.[1185]

d. Argument Under Statutory Factors

Proponents' analyses of the statutory factors are, once again, substantially the same for both Class 16 and Class 17.[1186] Under the first statutory factor, concerning the availability of copyrighted works, EFF notes that the smartphone market has only continued to grow throughout the duration of the existing exemption and suggests that "[t]he lack of an exemption would likely decrease the appeal of smartphones for many consumers and innovators."[1187] It notes that the Register previously concluded that jailbreaking increases the availability of smartphone software, "'while simultaneously being unlikely to interfere with the availability of smartphone operating systems.'"[1188] EFF urges that the same conclusion "holds true for other multipurpose devices."[1189]

EFF concedes that the second factor, which addresses nonprofit and educational concerns, is not relevant to this class, though it notes that "[t]he availability of mobile device firmware for nonprofit purposes will not be harmed by an exemption."[1190] On the third factor, pointing to examples of apps with political content that have been rejected from Apple's app store and the use of jailbroken smartphones to uncover security

[1180] EFF Class 16 Reply at 3; *see also* EFF Class 16 Supp. at 20 (noting that by giving the software administrative access to the operating system, those programs are given "more capabilities and more ability to interoperate with other programs").

[1181] *See* EFF Class 16 Supp. at 20 (citing Nexus and HTC authorized jailbreaking options); EFF Class 17 Supp. at 22 (same).

[1182] *Id.*

[1183] EFF Class 16 Supp. at 20-21; EFF Class 16 Reply at 4; *see also* Freeman Class 16 Reply at 1.

[1184] Freeman Class 16 Supp. at 3-4; Freeman Class 17 Supp. at 3-4.

[1185] EFF Class 16 Reply at 3.

[1186] *See, e.g.*, EFF Class 16 Supp. at 14-21; EFF Class 17 Supp. at 13-19.

[1187] EFF Class 16 Supp. at 20; EFF Class 17 Supp. at 22.

[1188] EFF Class 16 Supp. at 19 (quoting 2010 Recommendation at 102).

[1189] EFF Class 17 Supp. at 21.

[1190] EFF Class 16 Supp. at 21; EFF Class 17 Supp. at 23.

vulnerabilities, EFF asserts that "[m]obile device jailbreaking has spurred both valuable commentary and important security research."[1191]

On the fourth factor, concerning market impact, EFF argues that rather than harming the market for device firmware, "the proposed exemption is likely to stimulate the market for such works by providing developers with incentives to develop third party applications, thus making these devices—together with their copyrighted firmware—more attractive to consumers."[1192] EFF further maintains that "[t]he ability to jailbreak has never been shown to contribute significantly to copyright infringement."[1193] Finally, EFF argues that access controls on smartphones are not intended to protect copyrighted content but instead are intended to protect manufacturers' business interests, which is not a legitimate concern of copyright law.[1194]

2. Opposition

Opponents make somewhat different points with respect to Proposed Classes 16 and 17, so their arguments are treated separately.

a. Proposed Class 16: Jailbreaking – Wireless Telephone Handsets

BSA filed a brief comment in opposition to the exemption for smartphones.[1195] BSA argues that market alternatives to jailbreaking of smartphones obviate the need for an exemption. First, it points to EFF's statement that "Android devices, whether jailbroken or not, have long given users the ability to load application software from any source."[1196] BSA contends that this statement reveals that consumers have the ability to purchase mobile devices "that run an operating system that allows installation of applications obtained from virtually anywhere on the Internet."[1197] Second, BSA highlights EFF's concession that certain manufacturers have facilitated authorized jailbreaking, and argues that this constitutes a sufficient alternative to circumvention.[1198] BSA further notes that "phones are available without the restrictions that EFF describes," pointing to "developer editions" of phones offered by certain manufacturers.[1199]

[1191] EFF Class 16 Supp. at 21; *see also* EFF Class 17 Supp. at 17 (noting that Apple had rejected an app that "depicts the ongoing civil war in Syria" and one that "reports the locations of U.S. military drone strikes").

[1192] EFF Class 16 Supp. at 21; EFF Class 17 Supp. at 21-22.

[1193] EFF Class 16 Supp. at 21; EFF Class 17 Supp. at 23-24.

[1194] EFF Class 16 Supp. at 22 (citing 2010 Recommendation at 96-97; 2006 Recommendation at 152); EFF Class 17 Supp. at 24 (same).

[1195] BSA Class 16 Opp'n.

[1196] *Id.* at 2 (quoting EFF Class 16 Supp. at 20).

[1197] *Id.*

[1198] *Id.*

[1199] *Id.* at 2 & n.3.

In addition, BSA broadly observes that "circumvention related to mobile phones is detrimental to the secure and trustworthy innovative platforms that mainstream consumers demand."[1200] BSA claims that the first and fourth statutory factors in section 1201(a)(1) weigh against granting an exemption because "access controls have increased, rather than decreased, the availability of software applications designed for use on mobile phones" and also "preserve the 'market for and value of' legitimate software."[1201] BSA fails to elaborate on these points or cite supporting evidence, however. Nor does BSA respond to proponents' arguments that jailbreaking is a noninfringing use.

Finally, SAE Vehicle Electrical System Security Committee ("SAE VESS") requests that "vehicle-embedded computing devices" should be excluded from any exemption for Class 16.[1202] At the same time, however, SAE VESS acknowledges that an "automotive vehicle is not a wireless telephone handset device."[1203]

b. Proposed Class 17: Jailbreaking – All-Purpose Mobile Computing Devices

BSA filed somewhat more substantial comments in opposition to the exemption for general-purpose computing devices. First, BSA argues that, as in 2012, the Register cannot recommend the proposed exemption because EFF's definition of "'all-purpose mobile computing device'" is "amorphous" and provides "no principled basis by which to determine whether any particular device will be subject to the proposed exemption."[1204] BSA challenges in particular EFF's effort to distinguish between all-purpose mobile computing devices on the one hand, and laptops on the other. BSA notes that "the trend in personal computing is for distinctions that used to exist between tablets and laptops to disappear," as "[m]any laptops are sold with touch screens, cameras, and detachable keyboards," while "'hybrid' tablets, such as the Microsoft Surface, are designed to run substantially the same operating systems and range of software that laptops traditionally run."[1205] BSA also argues that there are a number of available alternatives to circumvention—such as use of Android devices that allow the use of applications from any source, or the use of laptops, which generally lack access controls.[1206]

BSA also urges that the statutory factors weigh against the exemption. With respect to the first factor, the availability for use of copyrighted works, BSA asserts that access controls "protect the investments companies and individual developers make in"

[1200] *Id.* at 1.

[1201] *Id.* at 2-3 (quoting 17 U.S.C. § 1201(a)(1)(C)(iv)).

[1202] SAE VESS Class 16 Reply at 2.

[1203] *Id.*

[1204] BSA Class 17 Opp'n at 2.

[1205] *Id.* at 2-3.

[1206] *Id.* at 4.

mobile devices, device firmware, and mobile applications.[1207] It claims that the "closed ecosystem" created by the use of TPMs "create[s] a reliable, secure platform that ultimately leads to the vast proliferation of copyrighted content because users come to expect a good experience."[1208] BSA argues that the second and third factors are not relevant, and that in any event EFF failed to support its claim that granting the exemption would further criticism and commentary.[1209] Finally, BSA argues that the fourth factor, regarding the effect of circumvention on the market for or value of copyrighted works, weighs against an exemption because "circumvention of access controls on tablets increases application piracy."[1210] In support of this last assertion, however, it cites a single 2012 news report about the shutdown of a store that sold pirated apps that could be installed on jailbroken iPhones and iPads.[1211]

General Motors ("GM"), the Alliance of Automobile Manufacturers ("Auto Alliance"), Motor & Equipment Manufacturers Association ("MEMA") and SAE VESS also filed comments under Class 17, all raising the same basic concern—that the class is framed in such a manner that it could arguably encompass computing systems that are embedded in "mobile" automobiles and other vehicles.[1212] In this regard, however, EFF clarifies that Class 17 "does not include software running on vehicle electronics" and that only portable devices—meaning devices designed to be carried or worn by a person—are meant to be encompassed by the class.[1213]

3. Discussion

The Register appreciates the significant consumer appeal of these proposed classes.[1214] Smartphones, tablets, and other all-purpose mobile computing devices are

---

[1207] *Id.*

[1208] *Id.*

[1209] *Id.* at 4-5.

[1210] *Id.* at 5.

[1211] *Id.* at 5 n.13 (citing Christopher MacManus, *Pirated iOS App Store Installous Shutters*, CNET (Dec. 31, 2012), http://www.cnet.com/news/pirated-ios-app-store-installous-shutters).

[1212] *See* GM Class 17 Opp'n at 3-4 ("[A]s drafted the Proponents' Class 17 could be construed to encompass in-vehicle telematics and communication systems . . . . [The Office] should narrow Class 17 to exclude in-vehicle telematics systems such as OnStar."); Auto Alliance Class 17 Opp'n at 1 (urging the Office "to ensure that vehicles are not inadvertently swept into the exemption"); MEMA Class 17 Reply at 1 ("The proposed exemption is . . . so broad that it may arguably include communications and in-vehicle telematics systems."); SAE VESS Class 17 Reply at 2 ("[I]f [t]he Librarian were to consider an exemption under this class 17 . . . then vehicle-embedded computers should be excluded from the list of devices for which this exemption applies.").

[1213] EFF Class 17 Reply at 2-3; *cf.* Tr. at 27:02-06 (May 21, 2015) (Lightsey, GM) (suggesting that inclusion of language stating that the device must be "portable" would exclude vehicles).

[1214] As previously mentioned, the Office received over 2000 individual submissions expressing support for Proposed Class 16, and nearly 1900 such submissions supporting Proposed Class 17. Additionally, attached to its reply comments, proponent EFF submitted a petition in support with over 20,000 signatures. EFF Class 16 Reply at App. A; EFF Class 17 Reply at App. A.

now a ubiquitous part of American life, and substantial numbers of device owners seek to take advantage of the existing smartphone jailbreaking exemption.[1215]

Based upon the current record, the Register concludes that proponents have successfully met their burden supporting an exemption for Classes 16 and 17. As explained, review in these proceedings is *de novo*, and proponents must therefore present persuasive evidence to support their case in each triennial rulemaking.[1216] The Register has explained, however, that where a legal analysis has previously been developed and no new law or arguments have been presented, the earlier legal determination can serve to support a renewed exemption, "provided that the evidence in the present record supports it."[1217] That principle is relevant here.

a. Noninfringing Uses

As noted, EFF argues that jailbreaking smartphones and all-purpose mobile computing devices for the purpose of running lawfully purchased software and the removal of unwanted software is likely to be a fair use. This argument is supported by the Register's reasoning in both the 2010 and 2012 rulemakings, both of which found, based on a review of the four fair use factors, that jailbreaking is likely to be a noninfringing fair use.[1218]

As suggested above, the parallel record permits a combined fair use analysis of jailbreaking of smartphones and other portable all-purpose mobile computing devices. Considering the first factor, the purpose and character of the use, the goal of jailbreaking is to allow the operating system on a device to interoperate with other programs, a favored purpose under the law.[1219] Even if this use is not considered transformative in nature—because the computer program is still being used for its intended purpose—that is not in and of itself a basis to reject a fair use claim. As the Register concluded in 2010 and 2012, even if a use is nontransformative, the first factor may nonetheless favor fair use where, as here, the purpose and character of the use is "noncommercial and personal" and enhances functionality.[1220]

Looking to the second fair use factor, also as in 2010 and 2012, the record establishes that the firmware modified in the course of jailbreaking to permit interoperability is largely functional, rather than expressive, in nature, thus weighing in favor of fair use.[1221] With regard to the third factor, the Register once again concludes

[1215] *See* Freeman Class 16 Supp. at 1; Freeman Class 17 Supp. at 1.

[1216] *See* 2012 Recommendation at 71; 2010 Recommendation at 14.

[1217] 2012 Recommendation at 71; *see also* 2006 Recommendation at 40.

[1218] 2012 Recommendation at 72-74; 2010 Recommendation at 92-100.

[1219] *See* 2012 Recommendation at 72; 2010 Recommendation at 93-95.

[1220] 2012 Recommendation at 72 (citing 2010 Recommendation at 93).

[1221] EFF Class 16 Supp. at 6; Freeman Class 16 Supp. at 6; *see also* 2012 Recommendation at 74; 2010 Recommendation at 95-97.

that, while jailbreaking often requires making a complete reproduction of the firmware, in light of the *de minimis* nature of the modifications ultimately made to the firmware to enable jailbreaking, this factor, while not favorable to fair use, is of limited relevance.[1222]

Finally, regarding the effect on the market value of the work, the Register noted in her 2012 recommendation that "the fourth factor calculus favors a fair use finding even more than it did in 2010," due to the evidence then presented that demonstrated the growth of the smartphone market during the period the previous exemption was in effect.[1223] The evidence in the current proceeding is much the same, with smartphone sales continuing to increase.[1224] This suggests that the market for smartphone firmware has not been harmed by jailbreaking. Furthermore, there is no reason on this record to reach a different conclusion for all-purpose mobile computing devices; opponents have put forth no evidence to demonstrate that the market for firmware or any other copyrighted works would be harmed by granting the jailbreaking exemption for all-purpose mobile devices. Thus, the fourth factor also favors fair use with respect to both of the proposed classes.

Accordingly, the Register concludes that proponents have met their burden of demonstrating that jailbreaking of smartphones and all-purpose mobile computing devices is likely to be a fair use.

Furthermore, the record of this proceeding shows that the category of "all-purpose mobile computing devices" has been meaningfully defined. To begin with, proponents suggest that the device must be portable or wearable. It also must be designed for general purpose computing rather than the consumption of a specific type of content. Although the Register appreciates BSA's point that the differences between tablet computers (which are included in the exemption) and laptops (which proponents did not seek to include and are thus excluded from the exemption) may be difficult to discern at the margins, this is not a reason to deny an exemption for all-purpose mobile computing devices.

The Register agrees with EFF's suggestion that a credible distinction can be made based on the type of operating system installed on the device.[1225] A device with an operating system that is primarily designed for mobile use, such as iOS, Android, or Windows RT, would be within the exemption, and those with operating systems designed primarily for desktop or laptop use, such as Windows 8 or Mac OS, would be outside it. If a hybrid device can act either as a laptop or a tablet, the user will need to investigate what type of operating system it contains in order to determine whether the exemption applies. To ensure sufficient guidance as to what is and is not covered, the Register proposes clarifying language for the tablet class, as discussed below.

[1222] 2012 Recommendation at 73-74; 2010 Recommendation at 96-97.

[1223] 2012 Recommendation at 74.

[1224] *See* EFF Class 16 Supp. at 2, 12-13; Chen Class 16 Reply at 1-2.

[1225] Tr. at 50:12-20 (May 21, 2015) (Stoltz, EFF).

b. Adverse Effects

Proponents have also established that a prohibition on jailbreaking would have an adverse impact on noninfringing uses of mobile device firmware protected by TPMs. The record shows that millions of consumers currently jailbreak their smartphones and that jailbreaking has facilitated a robust and profitable market for legitimate third-party software that cannot be used on non-jailbroken devices.[1226] The record also shows that jailbreaking can help ensure that older devices that may no longer be supported by their manufacturers are able to benefit from software updates, which may include fixes to security vulnerabilities.[1227] The record thus demonstrates that consumers will be adversely impacted if they are unable to engage in jailbreaking activities as a result of the prohibition on circumvention, because the inability to jailbreak will impede their ability to enhance the functionality, security, and longevity of smartphones and other devices.

The Register also concludes that alternatives to circumvention are inadequate to mitigate these adverse effects. Although Android is a somewhat more open platform than Apple's iOS in terms of the applications it will allow, the record shows that at least some functionalities may not be achievable unless an Android device is jailbroken, and it may not be possible to uninstall applications. The fact that some manufacturers have begun to authorize jailbreaking of certain devices or to sell already jailbroken devices does not alter this conclusion, as the record suggests that these phones and devices currently represent only a small fraction of the market.[1228]

c. Statutory Factors

Under the first statutory factor, the Register must consider the "availability for use of copyrighted works."[1229] As the Register noted in the 2010 and 2012 rulemakings, access controls prevent consumers from using third-party applications, so denying a jailbreaking exemption would significantly diminish the availability of those works.[1230] At the same time, granting the exemption is unlikely to discourage use or development of devices or the copyrighted firmware needed to run them.

As also noted in previous rulemakings, factor two, concerning the impact on nonprofit archival, preservation, and educational uses, does not appear to be directly implicated in these classes.[1231] Although in the past this has also been the conclusion for factor three, concerning the impact on criticism, comment, news reporting, teaching,

---

[1226] *See, e.g.*, EFF Class 16 Supp. at 20.

[1227] *See id.* at App A.

[1228] *See id.* (Statement of Dr. Jeremy Gillula at 2 n.2); EFF Class 16 Reply at 3-5; Freeman Class 16 Supp. at 3-4; Freeman Class 16 Reply at 1.

[1229] 17 U.S.C. § 1201(a)(1)(C)(i).

[1230] 2012 Recommendation at 76; 2010 Recommendation at 101.

[1231] *See* 17 U.S.C. § 1201(a)(1)(C)(ii)-(iii); 2012 Recommendation at 77; 2010 Recommendation at 101-102.

scholarship, or research, the Register notes that the current record suggests that jailbreaking may help further research of security flaws by allowing users to access a device's "lower-level functionality" to detect vulnerabilities.[1232]

As for the fourth factor, concerning the "effect of circumvention of technological measures on the market for or value of the copyrighted works,"[1233] there is no evidence on the current record that jailbreaking will harm the market for smartphones, devices, or the firmware within them. To the contrary, during the time that the jailbreaking exemptions for smartphones have been in place, the record shows that both the smartphone market and the market for independent apps have grown, while the manufacturer-authorized app market continues to thrive.[1234] There is no reason on this record to believe that a different result would obtain for all-purpose mobile computing devices, given that such devices operate in similar ways and with similar capabilities. The fourth factor therefore favors granting the proposed exemption.

4. NTIA Comments

NTIA proposes a jailbreaking exemption for all "mobile computing devices," a category which would include dedicated e-book readers separately addressed in Proposed Class 18 below.[1235] Quoting the Register's recommendation to exempt smartphone jailbreaking in 2010, NTIA stresses that "'[i]t does not and should not infringe any of the exclusive rights of the copyright owner to run an application program on a computer over the objections of the owner of the copyright in the computer's operating system.'"[1236] NTIA also notes that "the mobile applications market has thrived despite the existence of an exemption [for smartphone jailbreaking] for over five years."[1237]

NTIA believes that an exemption covering all "mobile computing devices"—including dedicated e-book readers and, apparently, other devices that are primarily designed for the consumption of particular content, such as handheld video game consoles—is warranted because "regardless of a device's particular form factor, the works and TPMs at issue are strikingly similar and many times identical."[1238] But NTIA does not cite any evidence that this fact is true with respect to dedicated e-book readers, handheld video game consoles, or other dedicated media consumption devices.[1239] Moreover, NTIA does not explain why it departs from EFF's original proposal, which

[1232] EFF Class 17 Supp. at 21, App. A (Statement of Marc Rogers at 1).

[1233] 17 U.S.C. § 1201(a)(1)(C)(iv).

[1234] BSA Class 16 Opp'n at 3; EFF Class 16 Supp. at 3, 12-13, 19; Chen Class 16 Reply at 2; Freeman Class 16 Supp. at 1.

[1235] NTIA Letter at 43-44.

[1236] *Id.* at 43 (quoting 2010 Recommendation at 96-97).

[1237] *Id.* at 45.

[1238] *Id.* at 44. NTIA states that it does not "intend to include vehicles in this exemption." *Id.* at 46.

[1239] *Id.* at 44 & n.203 (citing only evidence regarding smartphones and all-purpose mobile computing devices).

expressly excludes devices that are "designed primarily for the consumption of a single type of media," including "dedicated e-book readers."[1240] Accordingly, as discussed below, the Register recommends in favor of an exemption that reflects the proposals for Classes 16 and 17.

5. Conclusion and Recommendation

For the reasons described above, proponents of both Class 16 and Class 17 have satisfied their burden of showing that technological measures applied to smartphones and all-purpose mobile computing device software have an adverse effect on noninfringing uses. The statutory factors also tip in favor of granting the exemption.

As noted above, to address concerns regarding the scope of the category "all-purpose mobile computing device," the Register recommends several refinements to the proposed class, consistent with proponents' suggestions: the devices must be "portable," in the sense that they are designed to be carried or worn by individuals; they must be "designed to run a wide variety" of applications; and they must come "equipped with an operating system primarily designed for mobile use." The class thus excludes vehicle-embedded systems, devices designed primarily for consumption of a specific type of media (such as e-book readers and handheld gaming devices), and computers confined to desktop or laptop operating systems. The exemption also specifies that circumvention can be for the purpose of removing undesired software from the device. Finally, to simplify the language, the exemption substitutes "smartphone" for the less descriptive term "wireless telephone handset."[1241]

Accordingly, the Register recommends that the Librarian designate the following class:

> **Computer programs that enable smartphones and portable all-purpose mobile computing devices 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 smartphone or device, or to permit removal of software from the smartphone or device. For purposes of this exemption, a "portable all-purpose mobile computing device" is a device that is primarily designed to run a wide variety of programs rather than for consumption of a particular type of media content, is equipped with an operating system primarily designed for mobile use, and is intended to be carried or worn by an individual.**

[1240] EFF Jailbreaking Pet. at 2.

[1241] As previously noted, the term "wireless telephone handset" encompasses both phones that do and do not have the ability to run a wide range of software applications. The term is thus appropriately used in the context of the cellphone unlocking exemption in Class 11, since unlocking is potentially relevant to all types of mobile phones. Here, where the exemption is focused on interoperability of software applications, the Register uses the more descriptive term "smartphones."

F. Proposed Class 18: Jailbreaking – Dedicated E-Book Readers

1. Proposal

This class would allow circumvention of technological measures protecting dedicated e-book readers, such as Amazon's Kindle Paperwhite, to run lawfully acquired third-party applications or software on such devices. Maneesh Pangasa filed a petition seeking this exemption,[1242] and the NPRM described the class as follows:

> Proposed Class 18: This proposed class would permit the jailbreaking of dedicated e-book readers to allow those devices to run lawfully acquired software that is otherwise prevented from running.[1243]

Pangasa, however, failed to submit subsequent written comments or evidentiary materials in support of the petition or participate in the public hearings. Comments expressing general support for the proposed exemption were filed by the Free Software Foundation ("FSF"),[1244] Jay Freeman, the proprietor of an app store for jailbroken devices,[1245] Catherine Gellis and the Digital Age Defense project ("Gellis/Digital Age Defense"),[1246] and over 1600 individuals.[1247] The written comments provided no specific factual information in support of the exemption.[1248] Nor did they provide legal argument; no commenter explained why the proposed uses are noninfringing, how such uses are adversely impacted by the prohibition on circumvention, or why granting an exemption would be consistent with the statutory factors.

At the public hearing, Freeman briefly mentioned that people have jailbroken Kindle Paperwhite e-book readers to install screen savers or achieve broader functionality.[1249] But Freeman could not answer the significant question of whether the circumvention of TPMs protecting dedicated e-book readers would allow a user to access pirated books or other content on these platforms.[1250] This is just one of the many factors that would seem to be relevant to the consideration of Pangasa's proposal.

[1242] Pangasa Tablet Jailbreaking Pet. at 2 (seeking an exemption "extending the protections for (class #5) mobile phones to include . . . dedicated e-readers like the Amazon Kindle").

[1243] NPRM, 79 Fed. Reg. at 73,867.

[1244] FSF Class 18 Supp.

[1245] Freeman Class 18 Supp.

[1246] Gellis/Digital Age Defense Class 18 Supp.

[1247] Digital Right to Repair Class 18 Supp. (1608 individuals).

[1248] *See, e.g.*, FSF Class 18 Supp. at 1 (stating only that an e-book reader "should be under the control of the user"); Freeman Class 18 Supp. at 3 (This comment was written generally to apply to multiple jailbreaking classes, noting that "[a]n e-book reader . . . is 'only' an e-book reader . . . up until the moment that someone jailbreaks it: then it becomes like any other device.").

[1249] Tr. at 84:08-14 (May 21, 2015) (Freeman, SaurikIT).

[1250] *Id.* at 85:06-10 (Charlesworth, USCO; Freeman, SaurikIT) (discussing the "classic" Kindle and Nook).

Perhaps because of the lack of a written record in support of the proposed exemption, no opposition comments were filed.

2. NTIA Comments

As noted above in the discussion of Classes 16 and 17, covering smartphone and all-purpose mobile computing device jailbreaking, NTIA supports a jailbreaking exemption for all "mobile computing devices," a category which would presumably include dedicated e-book readers.[1251] NTIA, however, points to nothing in record to support a jailbreaking exemption for dedicated e-book readers. Instead, NTIA's analysis cites only evidence submitted for Classes 16 and 17, none of which supports an exemption for dedicated e-book readers.[1252] Indeed, EFF, the chief proponent of those classes, expressly excluded e-book readers from its proposal.[1253]

3. Conclusion and Recommendation

Pangasa and the supporters of this proposal have failed to provide meaningful evidentiary or legal support for Proposed Class 18. Because there is no record on which to assess whether the exemption satisfies the criteria set forth in section 1201(a)(1), the Register declines to recommend the adoption of Proposed Class 18.

[1251] NTIA Letter at 43-44.

[1252] *See id.* at 42-46.

[1253] EFF Jailbreaking Pet. at 2.

G. Proposed Class 19: Jailbreaking – Video Game Consoles

1. Proposal

Maneesh Pangasa filed a petition proposing an exemption to permit circumvention of TPMs on home video game consoles for an assortment of asserted noninfringing uses, including installing alternative operating systems and removing region locks.[1254] Such circumvention is often referred to as "jailbreaking." In general, access controls on video game consoles prevent the use of unauthorized video games. "Region locks" prevent the console from playing games from outside a particular geographic territory. The NPRM described the class as follows:

> Proposed Class 19: This proposed class would permit the jailbreaking of home video game consoles. Asserted noninfringing uses include installing alternative operating systems, running lawfully acquired applications, preventing the reporting of personal usage information to the manufacturer, and removing region locks. The requested exemption would apply both to older and currently marketed game consoles.[1255]

As discussed below, a similar exemption was considered and rejected in 2012 due to concerns about video game piracy.[1256]

Despite having submitted a petition, Pangasa failed to file supporting comments or participate in the public hearings. Short comments expressing general support for the proposed exemption were filed by iFixit,[1257] Free Software Foundation ("FSF"),[1258] Catherine Gellis and the Digital Age Defense project ("Gellis/Digital Age Defense"),[1259] and over 1600 individuals.[1260] None of the written comments, however, provided details about the TPMs or circumvention methods at issue or analyzed the statutory criteria for an exemption—*i.e.*, whether the proposed uses are noninfringing, whether the prohibition on circumvention was causing adverse effects, or whether an exemption would be justified under the factors set forth in section 1201(a)(1).

Moreover, the factual support offered by the supporting parties was scant and dated. In its brief written comments, iFixit cites a 2012 news article referring to the fact

---

[1254] Pangasa's petition sought an exemption ''for jail-breaking or rooting home video game consoles like Nintendo's Wii U, Sony's Play Station 4, Microsoft's Xbox One and home media devices like Apple TV which may in future gain the ability to natively play video games.'' Pangasa Video Game Console Jailbreaking Pet. at 1.

[1255] NPRM, 79 Fed. Reg. at 73,868.

[1256] 2012 Final Rule, 77 Fed. Reg. at 65,272-74.

[1257] iFixit Class 19 Supp.

[1258] FSF Class 19 Supp.

[1259] Gellis/Digital Age Defense Class 19 Supp.

[1260] Digital Right to Repair Class 19 Supp. (1647 individuals).

that, in an unspecified year, the U.S. Air Force networked 1700 PlayStation 3 consoles to use as a supercomputing platform, and that a researcher at the University of Massachusetts had used a grid of eight PlayStation 3 consoles to simulate gravitational waves.[1261] iFixit adds that "[u]sers of jailbroken consoles also have the ability to run 'homebrewed' [*i.e.*, independently developed] software," although it does not provide specific evidence regarding such activities.[1262]

iFixit's written comments make passing reference to jailbreaking for the purpose of repairing video game consoles, a topic on which iFixit's representative elaborated at the public hearing.[1263] At the hearing and in a post-hearing follow-up, iFixit urged that certain repairs might be less expensive if circumvention of access controls on the consoles were permitted, though it conceded that consoles can also be repaired without circumvention, including through official repair channels.[1264] For instance, iFixit described a malfunction on the Xbox 360 console known as the "red ring of death," but also acknowledged that this problem stemmed from a defect that could be repaired without circumvention.[1265]

iFixit also explained that, when the optical drive of a console fails, it may be challenging (though, as explained below, still feasible) to replace the drive without circumventing console TPMs because "the optical drives are cryptographically linked via their serial numbers to the motherboard" of the console.[1266] According to iFixit, by circumventing the TPMs, a user can modify the firmware on the motherboard to accept a new optical drive.[1267] But iFixit acknowledges that there are other methods of replacing a malfunctioning optical drive that do not require circumvention. First, the optical drive and the motherboard can be replaced at the same time.[1268] Second, it notes that the

---

[1261] *See* iFixit Class 19 Supp. at 3 (citing Jason Koebler, *Sony, Microsoft Battle Hackers Over Right to 'Jailbreak' Video Game Systems*, U.S. NEWS (Feb. 29, 2012), http://www.usnews.com/news/articles/2012/02/29/sony-microsoft-battle-hackers-over-right-to-jailbreak-video-game-systems).

[1262] *See id.*

[1263] *See id.* at 2; Tr. at 273:10-282:02 (May 20, 2015) (Wiens, iFixit; Charlesworth, USCO); Tr. at 275:22-24, Exhibit 6 (May 20, 2015) (Wiens, iFixit) (guide to repairing the Xbox 360 hardware error known as the "red ring of death").

[1264] Tr. at 282:03-286:06 (May 20, 2015) (Wiens, iFixit; Charlesworth, USCO; Damle, USCO); iFixit Post-Hearing Resp.

[1265] Tr. at 274:14-277:21 (May 20, 2015) (Wiens, iFixit; Charlesworth, USCO).

[1266] iFixit Post-Hearing Resp. at 2; *see also* Tr. at 281:02-282:07 (Wiens, iFixit; Damle, USCO).

[1267] iFixit Post-Hearing Resp. at 2. At the hearing, the representative for the Entertainment Software Association ("ESA") suggested that it may be possible to replace the firmware on the optical drive so that it matches an existing motherboard without the need for circumvention. Tr. at 305:19-306:02 (Frankel, ESA). In response to post-hearing questions posed by the Copyright Office, however, ESA and iFixit agreed that circumvention would be necessary to replace an entire optical drive. ESA Class 19 Post-Hearing Resp. at 1-3; iFixit Post-Hearing Resp. 1-2.

[1268] iFixit explains that, for a PlayStation 4, the cost of replacing both the optical drive and the motherboard would be about $200, while the cost of replacing just the optical drive (if circumvention were permitted) would be only about $100. Tr. at 282:08-24 (May 20, 2015) (Wiens, iFixit).

relationship between the drive and motherboard is not "one to one" and that there are a "number of different permutations of optical drives and [motherboards]."[1269] As a result, it is possible to replace just a malfunctioning optical drive, while keeping the existing motherboard, if one identifies a replacement drive that functions with that motherboard.[1270] iFixit urges, however, that finding a matching drive may be quite difficult, because the number of drive-to-motherboard permutations makes it difficult to stock the required parts.[1271] Third, iFixit acknowledges that, in addition to consoles still under warranty, the console manufacturers themselves provide official repair channels, noting that Sony will repair out-of-warranty PlayStation 3 consoles for a flat rate of $79, $99, or $129, depending on the edition of the console, and that Microsoft will repair out-of-warranty Xbox 360 consoles for a flat rate of $99.99 or $119.99, depending on "whether the repair is processed via an online portal or over the phone, respectively."[1272]

Proponents' assertions in this proceeding mirror claims made in the 2012 rulemaking. Just as iFixit does here, proponents in 2012 argued that jailbreaking would facilitate scientific research and homebrew activities.[1273] Indeed, with respect to those uses, proponents in 2012 relied on the same evidentiary examples that iFixit cites here.[1274] Like iFixit, the 2012 proponents also suggested that the "repair of outmoded gaming consoles" justified the jailbreaking exemption.[1275]

2. Opposition

Class 19 was opposed by ESA and Joint Creators.[1276] In brief, opponents urge the Register to recommend against adoption of the proposed exemption on the same grounds as in 2012.[1277] In particular, ESA asserts that "the ability to access and distribute infringing content is, in fact, a principal reason why users hack their video game consoles," and substantiates that claim with documentary evidence drawn from online forums and other sources that specifically describe jailbreaking as a means to allow users

[1269] *Id.* at 281:08-10 (Wiens, iFixit).

[1270] *Id.* at 281:11-283:11 (Wiens, iFixit; Damle, USCO).

[1271] *Id.* at 281:16-283:21 (Wiens, iFixit; Damle, USCO).

[1272] iFixit Class 19 Post-Hearing Resp. at 2-3.

[1273] 2012 Recommendation at 39.

[1274] *Id.* at 27 (noting that proponent cited "an Air Force project that made use of 1700 PS3s"); EFF, Comments Submitted in Response to the Sept. 29, 2011 Notice of Inquiry on the Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies 22 (Dec. 1, 2011), *available at* http://www.copyright.gov/1201/2011/initial/eff.pdf (noting that "an astrophysicist at the University of Massachusetts[] created complex simulations of gravitational waves using a grid of eight PS3s he developed as an alternative to more costly and inefficient methods of scientific research").

[1275] 2012 Recommendation at 31, 44.

[1276] The trade groups represented by Joint Creators are the Motion Picture Association of America, ESA, and the Recording Industry Association of America.

[1277] ESA Class 19 Opp'n; Joint Creators Opp'n.

to access unauthorized content on a console.[1278] Indeed, ESA asserts that "virtually all" video game console jailbreaking tools are "bundled with applications that permit users to play pirated content," a claim that is supported by documentary evidence from online sources.[1279] ESA thus urges that the primary effect of permitting users to jailbreak consoles would be to encourage piracy rather than the noninfringing uses cited by proponents.

Opponents also note that proponents rely on the same claimed harms that the Register deemed insufficient to support an exemption in 2012.[1280] With respect to the claim that jailbreaking video game consoles gives researchers access to affordable computing resources, ESA urges that "[n]eeding to spend fair market value for access to computing resources (as opposed to the below market cost of the video game console) is not the kind of harm that this rulemaking is intended to address."[1281] Moreover ESA notes the ready availability of other affordable computing resources, including "the emergence of 'cloud computing' and 'cloud service providers,' which have revolutionized access to scalable, customizable processing resources that can be continuously tailored to specific computing needs."[1282]

With respect to homebrew uses, opponents observe that there are a wide range of platforms on which to play independently developed games, including personal computers and Android devices.[1283]

Finally, ESA responds to iFixit's concerns about the ability to repair video game consoles by noting that all major console manufacturers offer repair services for both in-warranty and out-of-warranty consoles.[1284] In a post-hearing letter, ESA confirms that manufacturers of the Xbox 360 and PlayStation 3 consoles provide official repair services. Services for consoles under warranty "are offered at no charge to the customer."[1285] For out-of-warranty consoles, manufacturers also offer repair or replacement services ranging in price from $99 to $149.[1286] ESA argues that, to the

[1278] ESA Class 19 Opp'n at 3-4, Exhibit A; *see also* Joint Creators Class 19 Opp'n at 3-4.

[1279] ESA Class 19 Opp'n at Statement 1 at ¶ 9 (Statement of Dylan Rhoads), Exhibit A.

[1280] *Id.* at 8-9.

[1281] *Id.* at 9.

[1282] *Id.* at 10.

[1283] *Id.* at 11-12; Joint Creators Opp'n at 4.

[1284] ESA Class 19 Post-Hearing Resp. at 3-4.

[1285] *Id.* at 3; *see also id.* at 4.

[1286] For out-of-warranty consoles, manufacturers also offer repair services. According to ESA, for Xbox 360 consoles produced in or after 2008, Microsoft provides repair services for "a current flat fee of $99 for any hardware-related issues, including parts and labor;" while older models "are no longer supported," "[u]sed replacement consoles . . . are frequently sold for well under $99" via online marketplaces such as eBay. *Id.* at 4. ESA explains that Sony Computer Entertainment America ("SCEA") provides repair services for all models of the PlayStation 3 except three early models; for those older models, however,

extent proponents claim that repair through official channels is more difficult or expensive than engaging in circumvention, this does not provide a basis for an exemption.[1287]

3. NTIA Comments

NTIA recommends in favor of a video game console jailbreaking exemption limited to "the purpose of repairing malfunctioning hardware, for systems that are obsolete or no longer covered by manufacturer warranty."[1288] In NTIA's view, "[t]he record indicates that circumvention is sometimes necessary to effectively perform . . . repairs," and that "[c]onsole owners may need to perform repairs well after warranty coverage has expired."[1289] NTIA maintains that alternatives to circumvention are inadequate because "[m]ost of those alternatives require the owner to submit the console to the manufacturer and, in some circumstances, pay a substantial fee to repair the item if the warranty has expired."[1290]

At the same time, NTIA concludes that a broader exemption to allow for the installation of alternative software and third-party applications is not warranted "due to an insufficient record." Indeed, according to NTIA, "the current record to support [such an] exemption is significantly less robust and detailed than it was in the last rulemaking."[1291]

As discussed below, the Register concludes that the current record does not support an exemption for jailbreaking of video game consoles, even one limited to console repair. The evidence shows that consoles can be repaired without the need to engage in circumvention.

4. Conclusion and Recommendation

In 2012, the Register determined that "access controls on gaming consoles protect not only the console firmware, but the video games and applications that run on the console as well," many of which are owned by the console manufacturers.[1292] Based on extensive record evidence provided by opponents in that proceeding, the Register concluded that "the circumvention of console restrictions—even when initially undertaken for salutary purposes—is inextricably linked to and tends to foster piracy."[1293]

SCEA "offers a replacement model for $149 where the consumer is not required to send in the older unit, or [a] $99 exchange for a newer model." *Id.* at 3.

[1287] *Id.* at 4-5.

[1288] NTIA Letter at 49.

[1289] *Id.* at 48

[1290] *Id.* at 48-49.

[1291] *Id.* at 48.

[1292] 2012 Recommendation at 41.

[1293] *Id.* at 43.

She further concluded that "circumvention of access controls to permit interoperability of video game consoles—regardless of purpose—has the effect of diminishing the value of, and impairing the market for, the affected code, because the compromised code can no longer serve as a secure platform for the development and distribution of legitimate content."[1294] The Register thus determined that proponents had "failed to fulfill their obligation to establish persuasively that fair use can serve as a basis for the exemption they seek."[1295]

The Register additionally determined in 2012 that proponents had failed to satisfy their burden to show that the claimed noninfringing uses were adversely affected by the prohibition on circumvention. The record there referenced three academic research projects and one military project that employed video game consoles instead of all-purpose computers.[1296] But this showing did not change the fact that "alternative computing resources for such projects are available in the marketplace."[1297] The record also demonstrated that there were relatively few users of "homebrew" video game programs[1298] and that, in any event, "independent development of video games and other applications can be pursued on thousands of other Linux-based devices and other platforms, as well as through various programs offered by the console manufacturers themselves."[1299] Finally, the Register also found in 2012 that proponents had failed to substantiate their claim that the prohibition on circumvention was impeding repair of outmoded consoles.[1300]

In this rulemaking, proponents have failed to offer a legal or factual basis to support a different outcome here. Proponents have not provided any legal analysis, let alone an explanation of why the Register's legal conclusions should be different now than in 2012. The sparse evidence proffered by proponents in this proceeding is not materially different from the evidence considered in 2012. At the same time, opponents have provided substantial evidence to support the conclusion that jailbreaking of video game consoles leads to infringing activity and that there continue to be readily available alternatives to circumvention for each of the activities proffered by proponents.

Although the record in this proceeding is somewhat more developed with respect to the issue of console repair, it still does not support the need for an exemption. The major game console manufacturers appear to offer repair services for in- and out-of-warranty consoles either for free or at reasonable prices. Moreover, the record shows that

[1294] *Id.* at 44.

[1295] *Id.*

[1296] *Id.* at 45-46.

[1297] *Id.* at 47.

[1298] *Id.* (noting that "some homebrew applications attract only thousands of users, or fewer, from the tens of millions of console owners").

[1299] *Id.*

[1300] *Id.*

proponents themselves are able to offer repair services without the need to circumvent. Proponents did not provide any examples of an actual inability to repair a console through one of these means.

Accordingly, the Register recommends against adoption of Proposed Class 19.

H. Proposed Class 20: Jailbreaking – Smart TVs

1. Proposal

In addition to their traditional functionality, many modern televisions ("TVs") have built-in software features that can stream content over the internet, interact with other devices in the home, or run applications.[1301] The Software Freedom Conservancy ("SFC") proposed an exemption to permit circumvention of access controls on firmware (*i.e.*, the operating system) of such internet-enabled TVs—often referred to as "smart TVs"—to enable installation of third-party software.[1302] According to SFC, third-party software applications can allow a smart TV to interoperate with local computer networks and external peripherals, access media stored on external storage devices, and improve the TV's accessibility features.[1303] The NPRM described the class as follows:

> Proposed Class 20: This proposed class would permit the jailbreaking of computer-embedded televisions (''smart TVs''). Asserted noninfringing uses include accessing lawfully acquired media on external devices, installing user-supplied licensed applications, enabling the operating system to interoperate with local networks and external peripherals, and enabling interoperability with external devices, and improving the TV's accessibility features (*e.g.*, for hearing-impaired viewers). The TPMs at issue include firmware encryption and administrative access controls that prevent access to the TV's operating system.[1304]

Along with SFC, comments supporting Proposed Class 20 were filed by Free Software Foundation ("FSF"),[1305] Catherine Gellis and the Digital Age Defense project ("Gellis/Digital Age Defense"),[1306] The Exploiteers, which described itself as a "group of hobbyist security researchers,"[1307] and Jay Freeman, who runs an app store for jailbroken

---

[1301] *See* SFC Pet. at 3; The Exploiteers Supp. at 1.

[1302] SFC's proposal was to ''permit owners of computer-embedded televisions ('Smart TVs') to circumvent firmware encryption and administrative access controls that control access to the TVs' operating systems, for the purpose of accessing lawfully-acquired media, installing licensed applications, and enabling interoperability with external devices.'' SFC Pet. at 1.

[1303] *Id.* at 2.

[1304] NPRM, 79 Fed. Reg. at 73,868.

[1305] FSF Class 20 Supp.

[1306] Gellis/Digital Age Defense Class 20 Supp.

[1307] The Exploiteers Supp. at 1. In its brief comments, The Exploiteers also asked that Class 20 be extended to "streaming media players," such as the Logitech Revue, Google Chromecast, and Boxee Box. *Id*. No record was made, however, to support a jailbreaking exemption for such devices. The petition filed by SFC—the sole party to offer substantive legal argument and factual evidence in support of Proposed Class 20—was limited to smart TVs, as were all of SFC's later submissions.

devices.[1308] In addition, over 1700 individuals filed comments in support of Proposed Class 20.[1309]

a. Background

According to SFC, manufacturers of smart TVs restrict access to the TV's firmware using two types of TPMs. First, the firmware may be encrypted on the smart TV. To circumvent that encryption scheme, a user must first obtain a copy of the smart TV's firmware by obtaining a firmware update from the manufacturer that contains an entire copy of the firmware.[1310] Because the firmware update is also encrypted, the user must then decrypt the update. According to SFC, "[d]ifferent encryption schemes are used by different manufacturers (and on different TVs produced by a single manufacturer)."[1311] SFC explains, however, that most encryption schemes "involve the application of a well-known encryption algorithm such as Advanced Encryption System (AES), in conjunction with a secret key selected by the manufacturer."[1312]

SFC further explains that in some cases, "[s]mart TV modification enthusiasts have discovered the 'secret key' by 'brute force,' i.e. by using a program to guess every possible key until the correct key is found, yielding the ability to decrypt the contents of updates."[1313] Once the firmware is decrypted, a user can make any desired modification to that firmware, including adding new applications. The firmware update can then be re-encrypted using the manufacturer's specified scheme. When the update is installed on the smart TV, the modified firmware and new applications are then available on the smart TV.[1314]

Further, smart TVs may include "administrative access controls" that limit users' ability to install or execute applications. To bypass these access controls, "it is often necessary to identify and exploit a security vulnerability exposed by an application installed on the TV."[1315] SFC explains, for example, that "the administrative access controls employed by certain models of Sony Bravia Smart TVs can be circumvented by causing the TV to run a program that exploits a memory error to give the user administrative access."[1316] According to SFC, "[t]his is the same type of technique used to jailbreak many smartphones, an activity for which an exemption has been granted."[1317]

[1308] Freeman Class 20 Supp. at 1.

[1309] *See* Digital Right to Repair Class 20 Supp. (1724 individuals).

[1310] SFC Supp. at 1-4.

[1311] *Id.* at 3.

[1312] *Id.*

[1313] *Id.*

[1314] *Id.*

[1315] *Id.* at 4.

[1316] *Id.*

[1317] *Id.*

SFC notes as well that access to copyrighted media or works displayed or played on smart TVs "is controlled by separate TPMs" from those used to protect the smart TV firmware.[1318] At the public hearing, SFC elaborated on this point, explaining that "smart TVs are typically mostly platforms for streaming content from providers such as Netflix or Amazon or Hulu and those providers provide their own applications that embed their own encrypted stream handling."[1319] SFC thus expressed its understanding that circumventing the TPM protecting the firmware of a smart TV "does not weaken or affect . . . the TPM that is separately on Netflix."[1320]

b. Asserted Noninfringing Uses

SFC explains that although smart TV manufacturers place TPMs on the firmware as a whole, the "overwhelming majority" of that firmware incorporates the manufacturer's own proprietary applications along with free, libre, and open source software ("FLOSS") applications produced by third parties.[1321] These open source applications are licensed under terms that give anyone broad rights to use, copy, modify, and distribute the software.[1322] SFC asserts that, under the relevant FLOSS licenses, smart TV owners "are explicitly permitted to access these applications, modify their functionality, and install new or modified versions of the applications onto their TVs."[1323] For example, according to SFC, "[t]he flagship Smart TVs of the top manufacturers—Samsung, Sony, and LG—all run operating systems based on Linux."[1324] Linux is licensed under the General Public License ("GPL"), a FLOSS license which "permits recipients of the software to obtain the software's source code and to copy, modify, and redistribute the software without [a] fee (and requires distributors of the software to extend these rights to recipients)."[1325] SFC further explains that "[t]he GPL's terms permit television manufacturers to use GPL-licensed software in their Smart TVs, but they also ensure that consumers who purchase TVs containing that software have the right to modify it and to run it without restriction."[1326]

[1318] *Id.* at 10.

[1319] Tr. at 121:10-14 (May 20, 2015) (Williamson, SFC).

[1320] *Id.* at 124:18-23 (Damle, USCO; Williamson, SFC).

[1321] SFC Supp. at 1-2, 4; *see also id.* at 13-15 (list of FLOSS software components used by major smart TV manufacturers); *id.* at 38 (photograph of open source license notification on Samsung smart TV).

[1322] *Id.* at 2.

[1323] *Id.* at 4-5.

[1324] SFC Pet. at 2.

[1325] *Id.*; *see also* SFC Supp. at 17 (version 2 of the GPL) ("These [license] restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it . . . . For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights you have. You must make sure that they, too, receive or can get the source code."); SFC Supp. at 25 (version 3 of the GPL).

[1326] SFC Pet. at 2.

Accordingly, with respect to the FLOSS applications that are incorporated into smart TV firmware, SFC asserts that circumvention of the access controls on the firmware would permit licensed, and therefore noninfringing, uses of those applications.

Although SFC asserts that installation of third-party applications typically only requires access to, and presumably modification of, FLOSS firmware applications,[1327] it acknowledges that jailbreaking may also require access to proprietary, non-FLOSS firmware applications found in some smart TVs.[1328] With respect to those proprietary applications, SFC invokes fair use as a basis for making the necessary reproductions and modifications to permit installation and execution of lawfully acquired programs.[1329] Although SFC does not specifically analyze the four statutory fair use factors, it cites *Sega Enterprises Ltd. v. Accolade, Inc.*[1330] and *Lexmark International, Inc. v. Static Control Components, Inc.*[1331] in support of the proposition that "[c]opyright law recognizes that an owner's access to and modification of software to allow interoperability is fair use."[1332]

Related to the question of fair use, SFC disputes opponent Joint Creators's argument, discussed below, that the Federal Circuit's decision in *Oracle America, Inc. v. Google Inc.*[1333] should change prior reasoning of the Register that facilitating interoperability may be considered a non-infringing use for purposes of an exemption. SFC argues that *Oracle v. Google* is distinguishable. SFC observes that the case was principally about the copyrightability of certain code, and that SFC "does not question the copyrightability of code or applications."[1334] Furthermore, SFC argues that the decision has no bearing on its fair use claim because the court of appeals remanded the fair use issue for further consideration.[1335] SFC also notes that the Federal Circuit did not overrule the Ninth Circuit's decisions in either *Sega*[1336] or *Sony Computer Entertainment,*

[1327] *Id.* SFC explains, for instance, that "on some Smart TV models, once the owner has circumvented the firmware encryption, they can enable the TV to connect to other devices on their local network simply by causing the FLOSS operating system to run a FLOSS application (a telnet server) when it starts up." *Id.* at 2-3.

[1328] SFC Supp. at 2.

[1329] *Id.* at 5-7.

[1330] 977 F.2d 1510 (9th Cir. 1992).

[1331] 387 F.3d 522 (6th Cir. 2004).

[1332] SFC Supp. at 7 & nn.33-34 (citing *Sega*, 977 F.2d at 1528 and *Lexmark*, 387 F.3d at 550-51). SFC also makes a passing reference to section 117(a)(1), which permits the owner of a copy of a computer program to make a copy or adaptation of a computer program under certain circumstances. 17 U.S.C. § 117(a). Because SFC provides no evidence to demonstrate that the owner of a smart TV owns, rather than licenses, the copy of proprietary applications included in the smart TV's firmware, as required to invoke section 117, the Register analyzes only SFC's fair use claim.

[1333] 750 F.3d 1339 (Fed. Cir. 2014).

[1334] SFC Reply at 5.

[1335] *Id.*

[1336] 977 F.2d 1510.

Inc. v. Connectix Corp.,[1337] both of which treated uses necessary to enable interoperability as fair uses.[1338]

c. Asserted Adverse Effects

SFC points to several adverse effects resulting from section 1201(a)(1)'s prohibition on circumvention.[1339] First, SFC notes that it is "primarily concerned with facilitating the use of FLOSS applications produced by its member projects and other FLOSS community members."[1340] SFC explains that, in general, the goal of section 1201 is to give copyright owners control and circumscribe the use of their works.[1341] Smart TV manufacturers, however, do not own the copyright in the FLOSS applications included in the firmware. By nevertheless installing TPMs on those TVs that limit access to the firmware as a whole, SFC suggests that those manufacturers are frustrating the wishes of the copyright owners of FLOSS applications, who chose to license their software on terms specifically allowing broad access to and modification of their works.[1342]

Second, SFC asserts that the TPMs adversely affect the ability to enable the smart TV firmware (and the TV itself) to interoperate with third-party software and devices. SFC notes that some independent developers have created a number of applications to modify the behavior of jailbroken TVs. For instance, SFC cites the SamyGo project, which distributes software for Samsung-branded TVs that performs functions such as "modify[ing] subtitles to be larger, brighter, or outlined to enhance readability," "enabl[ing] or expand[ing] the TV's compatibility with peripheral hardware, such as mice, keyboards, and external storage devices," and "chang[ing] the aspect ratio, resolution, or scale of the TV's display."[1343] According to SFC, by prohibiting the jailbreaking of smart TVs to permit the installation of these independently developed applications, section 1201(a)(1) "limits creativity and the production of new copyrighted works."[1344]

SFC also notes that many of these enhancements "make the TVs more accessible to people with disabilities"—such as "text-to-speech applications to read subtitles aloud to sight-impaired users"—or enable smart TVs to "work with accessibility products such

[1337] 203 F.3d 596 (9th Cir. 2000).

[1338] SFC Reply at 5.

[1339] The Register notes that proponents do not address the reverse engineering or encryption exemptions under section 1201. *See, e.g.*, 17 U.S.C. § 1201(f), (g). However, as observed by the Register in other contexts, these exemptions are unlikely to cover the full range of activities at issue. *See* 2010 Recommendation at 94 & n.318, 199.

[1340] SFC Supp. at 4.

[1341] *Id.* at 6.

[1342] *Id.* at 6-7

[1343] *Id.* at 5.

[1344] *Id.* at 7.

as headphones [or] powered neckloop devices."[1345] In response to a claim by opponent LG Electronics U.S.A., Inc. ("LG"), discussed below, that LG-manufactured smart TVs already contain many accessibility features, SFC testified that TVs made by other manufacturers lack such accessibility features.[1346]

SFC also suggests that there is no viable alternative to circumvention because "[t]here is no other way to access the firmware and filesystem on which [FLOSS software is] installed."[1347] SFC rejects the suggestion that connecting a laptop to the TV is a viable alternative to circumvention because this solution does not permit users to access the FLOSS software they are entitled to access, and does not permit the installation of software to enhance the operation of the TV itself.[1348]

d. Argument Under Statutory Factors

SFC argues that the proposed exemption is supported by each of the statutory factors. First, it argues that the exemption would enhance the availability for use of copyrighted works by allowing users to access FLOSS applications running on smart TVs, and to make modifications to those applications that will themselves become available to other users—and to manufacturers—under the applicable FLOSS license.[1349] In addition, SFC claims that the exemption would "increase the availability of third-party applications . . . that are designed to run on Smart TVs and enhance their functionality."[1350] At the same time, SFC argues that the availability of smart TV firmware itself will not be adversely affected, because "[t]here is no market for Smart TV firmware sold separately from the TVs themselves" and "the proprietary software on Smart TVs would be useless if separated from the TV it is intended to run on."[1351] In particular, SFC notes that firmware "exists on the TV in compiled, object code form" that is "compiled for the specific hardware architecture and software environment of the TV it runs on."[1352] According to SFC, "[d]ivorced from that environment, [the firmware] cannot be used."[1353]

Second, SFC claims that the exemption will enhance the availability of works for nonprofit educational uses. It argues that giving users access to the FLOSS applications

---

[1345] *Id.* at 5-6. A powered neckloop is a device that can connect a TV or other device to a hearing aid. *See Clearsounds Quattro Amplified Bluetooth Neckloop*, CLEARSOUNDS, https://www.clearsounds.com/product/quattro-40-adaptive-bluetooth-system (last visited Oct. 7, 2015) (cited in SFC Supp. at 6 n.24).

[1346] Tr. at 132:11-133:08 (May 20, 2015) (Williamson, SFC).

[1347] SFC Supp. at 7.

[1348] *See* SFC Reply at 4.

[1349] SFC Supp. at 7.

[1350] *Id.*

[1351] *Id.* at 8.

[1352] *Id.*

[1353] *Id.*

installed on smart TVs will further "[o]ne of the fundamental purposes of the [GPL] and other FLOSS licenses," which is "to give users the freedom to study and learn from the software they use."[1354] Third, SFC argues that the exemption would further "criticism, comment, news reporting, teaching, scholarship, [and] research" by "enabl[ing] researchers to find and expose security and privacy issues in Smart TVs."[1355] SFC states that "Smart TVs have been shown to contain security vulnerabilities that can be exploited by malicious hackers to access them remotely and run harmful code," including vulnerabilities that "make use of a Smart TVs' built-in microphone and camera."[1356]

Fourth, SFC argues that circumvention will not have an adverse effect on the market for or value of copyrighted works. It notes that circumvention would facilitate a market for third-party software, including FLOSS software that can benefit the manufacturers themselves, who would "have the right under the applicable FLOSS license to use these modifications in their products."[1357] SFC explains that permitting circumvention could enhance the market for smart TVs by making them more useable and increasing the demand for more customizable TVs.[1358] SFC also stresses that circumvention "would neither impact the availability of copyrighted media or works displayed or played on Smart TVs nor encourage infringement of them," because, as described above, "[a]ccess to this content is controlled by separate TPMs."[1359]

SFC makes several points in response to the claim, discussed below, that jailbreaking a smart TV would enable piracy. SFC emphasizes that its petition "does not propose, and would not enable, circumvention of the Digital Rights Management ('DRM') systems and other TPMs" controlling access to copyrighted works that are played on smart TVs.[1360] SFC maintains that opponents have provided no evidence that jailbreaking would enable piracy of proprietary applications installed on smart TVs. SFC notes that "even if a proprietary application . . . was extracted from an unlocked Smart TV, it could not be trivially shared in the same way software on a personal computer can be."[1361] According to SFC, that is because "[t]he hardware architecture of Smart TVs often var[ies] significantly from one model to the next, and each application must be compiled for the architecture of the TV it is intended to run on—if it was copied to a TV with a different architecture, it simply wouldn't run."[1362]

[1354] *Id.*

[1355] *Id.*

[1356] *Id.* at 9.

[1357] *Id.*

[1358] *Id.* at 9-10.

[1359] *Id.* at 10.

[1360] SFC Reply at 2.

[1361] *Id.*

[1362] *Id.*

With respect to other factors that the Librarian should consider, SFC argues that the exemption would "give users a means to extend the effective lifespan of their Smart TVs" by allowing them to "add features to their TVs rather than purchase a new one" that has those features.[1363] SFC gives the example by analogy of the Linksys WRT54G router, which SFC claims was on the market for a longer period of time than nearly any other consumer router because it permitted installation of "FLOSS community firmware . . . which unlocked latent capabilities that the manufacturer did not provide."[1364]

SFC disputes LG's claim, addressed below, that permitting jailbreaking would harm "platform security" by making smart TVs more vulnerable to malicious software or hacking. SFC acknowledges that "to some extent these TPMs are primarily designed for systems security," specifically, to "prevent unauthorized software from being installed inadvertently or against the user's wishes."[1365] SFC also acknowledges LG's suggestion that a jailbroken TV might not receive further manufacturer-authorized updates.[1366] But SFC expresses doubt that "these TVs are updated so frequently or for such a long period by the manufacturers that they really are kept much safer by keeping them in the stock configuration."[1367] Moreover, SFC emphasizes that ultimately, "[t]he user is making an active choice to stop receiving those updates in order to have access to more functionality on the television."[1368]

SFC also suggests that, in at least some cases, the exemption under consideration would not make smart TVs more vulnerable to unwanted software because the TPMs on the TV would not be eliminated by the circumvention process.[1369] To support that claim, SFC points specifically to the fact that, as noted above, the circumvention of the encryption-type TPMs takes place externally to the TV, using an encrypted firmware update; the encryption checks on the TV ultimately remain in place.[1370] Accordingly, SFC suggests, any unwanted software would continue to be blocked by the encryption scheme. By contrast, however, SFC did not address whether the alternative method of circumvention, involving bypass of administrative access controls, would similarly leave the relevant protections in place.

[1363] SFC Supp. at 10.

[1364] *Id.*

[1365] Tr. at 129:06-12 (May 20, 2015) (Williamson, SFC).

[1366] *Id.* at 130:16-20 (Williamson, SFC).

[1367] *Id.* at 131:22-25 (Williamson, SFC).

[1368] *Id.* at 131:14-16 (Williamson, SFC).

[1369] *Id.* at 129:13-130:15 (Williamson, SFC).

[1370] SFC Supp. at 10.

2. Opposition

Proposed Class 20 was opposed by Joint Creators[1371] and LG.[1372]

a. Asserted Noninfringing Uses

Opponents do not appear to take issue with proponents' assertion that much of the computer code embedded by manufacturers in smart TVs may be accessed and altered by TV owners because it is subject to FLOSS open source licenses.[1373] Joint Creators, however, dispute proponents' invocation of fair use as a basis for copying and modifying the non-FLOSS proprietary software in smart TVs, although they do not engage in specific analysis of the four fair use factors. While acknowledging the Register's earlier determinations that jailbreaking of smartphones to permit independently created software applications to run is likely to be a fair use, they offer two reasons why the same logic does not extend to smart TVs.[1374]

First, Joint Creators assert that proponents "have not described in any detail the process of circumventing access controls used on computer programs resident on smart TVs," and that proponents have therefore not met their burden of demonstrating that the exemption would facilitate a noninfringing use.[1375] Joint Creators do not explain, however, how this argument ties into the fair use analysis. Second, Joint Creators invoke the Federal Circuit's decision in *Oracle v. Google*.[1376] In that case, the lower court had held that the "declaring code" of software packages written in the Java programming language was uncopyrightable, in part based on its conclusion that copying that code was necessary to enable interoperability with other software written in the Java programming language.[1377] The Federal Circuit reversed, rejecting the argument that there is an "interoperability exception" to copyrightability.[1378] While acknowledging that fair use was a separate issue that was not finally decided by the Federal Circuit, Joint Creators nevertheless claim that the decision "calls into question the Register's reasoning from

---

[1371] Joint Creators Class 20 Opp'n. The trade groups represented by Joint Creators are the Motion Picture Association of America, the Entertainment Software Association, and the Recording Industry Association of America.

[1372] LG Reply. The Register notes that LG filed its comments in the reply phase of the written comment period, which had been designated as allowing proponents and neutral commenters to respond to points made by the opposition. Because only two comments were filed in opposition to this proposed class, the Register will exercise her discretion to consider LG's comments in reply, while at the same time being mindful that proponents did not have an opportunity to file written comments in response to LG.

[1373] *See* Joint Creators Class 20 Opp'n at 3-4 (in considering the TPMs and asserted noninfringing use at issue, Joint Creators do not attempt to rebut the claim that much of the code in smart TVs is subject to an open source license).

[1374] *Id.* at 3 (citing 2012 Recommendation at 72, 74); *see also* 2010 Recommendation at 92-94.

[1375] Joint Creators Class 20 Opp'n at 3.

[1376] 750 F.3d 1339.

[1377] *Oracle Am., Inc. v. Google Inc.*, 872 F. Supp. 2d 974, 976-77 (N.D. Cal. 2012).

[1378] *Oracle v. Google*, 750 F.3d at 1370.

prior cycles" that jailbreaking smartphones to enable interoperability is likely to be a fair use.[1379]

b. Asserted Adverse Effects

Joint Creators assert that any of the adverse effects claimed by proponents of the exemption are mitigated by the availability of laptop computers that "can be connected to television sets such that the output of these applications would be viewable on television screens," noting that a laptop is "capable of running whatever applications the proponents would like to develop and run."[1380]

LG, for its part, suggests circumvention is unnecessary because LG smart TVs already provide all of the features that SFC claims can be added only by jailbreaking smart TVs, including the ability to modify subtitles and to change the aspect ratio, to accommodate people with disabilities, and to connect to peripheral hardware such as mice and keyboards.[1381]

c. Argument Under Statutory Factors

Under the first statutory factor, "the availability for use of copyrighted works,"[1382] Joint Creators urge that an exemption would undermine the dissemination of legitimate applications and creative content. Joint Creators argue that "the platforms and devices that smart TV manufacturers and software providers design not only provide software developers and consumers with reliable ecosystems within which to offer innovative new products, but they also prevent application piracy by proactively excluding infringing applications."[1383] Joint Creators note that not only can "applications that themselves are infringing copies of other applications" be installed on jailbroken TVs, but "applications that infringe other types of works such as movies and television shows" can also be installed.[1384] Joint Creators point in particular to the application "Popcorn Time," which uses the BitTorrent protocol to facilitate viewing of pirated movies and TV shows.[1385] According to an article submitted by Joint Creators, Popcorn Time has millions of users and has "made BitTorrent piracy as easy as Netflix, but with far more content and none of those pesky monthly payments."[1386]

[1379] Joint Creators Class 20 Supp. at 4.

[1380] *Id.*

[1381] LG Reply at 3.

[1382] 17 U.S.C. § 1201(a)(1)(C)(i).

[1383] Joint Creators Class 20 Opp'n at 4-5.

[1384] *Id.* at 5.

[1385] *Id.*

[1386] *Id.* at Exhibit 2 (reproducing Andy Greenberg, *Inside the Popcorn Time, The Piracy Party Hollywood Can't Stop*, WIRED (Mar. 18, 2015), http://www.wired.com/2015/03/inside-popcorn-time-piracy-party-hollywood-cant-stop).

LG also disputes SFC's claim under the first statutory factor that the exemption would enhance the availability of copyrighted works, noting that LG "not only provides its users with extensive availability to [sic] third party applications, but also provides open-source programs which allow users to connect with other external devices and applications."[1387]

Under the second statutory factor, LG takes issue with SFC's claim that having access to FLOSS applications will enable users to study and learn from open source software. LG states that "it cannot be assumed that all users will be utilizing the capability to study the design and formation of copyright protected software merely for educational purposes," and that some users "will utilize these capabilities to copy and infringe on another's copyright[] protected property."[1388] Under the third factor, LG challenges SFC's proposition that allowing circumvention would spur research, comment, and reporting on security and privacy issues in smart TVs. LG states that it "provides a number of means for consumers to communicate their concerns or any defects that may exist in a television's system."[1389]

Under the fourth factor, Joint Creators argue that allowing jailbreaking would undermine the "market for and value of copyrighted works"[1390] by enabling piracy of smart TV applications and permitting installation of applications that can be used to consume pirated content.[1391] LG similarly asserts that "this exemption would restrict the ability of LG and other Smart TV manufacturers from developing Smart TV services with content owners and distributors, such as Amazon, Hulu, Netflix, and additional content distributors of all sizes since circumvention would expose their products to infringing users and unauthorized distribution."[1392] But LG and Joint Creators do not dispute SFC's assertion that streaming services that are accessed via smart TVs have TPMs that operate separate and apart from the TPMs on the smart TV firmware.

Finally, LG also expresses concern that "[a]llowing this exemption would affect the value of the product and dilute the LG brand," and it specifically references "OpenLGTV," an unauthorized reverse-engineering project that creates third-party applications for jailbroken LG smart TVs.[1393] LG expresses concern that "many consumers that may come across OpenLGTV are likely to be unaware that OpenLGTV is not affiliated with their LG Smart TV before permanently altering their television."[1394] Under the fifth statutory factor—concerning such other factors as may be appropriate for

[1387] LG Reply at 4.

[1388] *Id.*

[1389] *Id.*

[1390] 17 U.S.C. § 1201(a)(1)(C)(iv).

[1391] Joint Creators Class 20 Opp'n at 5.

[1392] LG Reply at 4.

[1393] *Id.* at 5; *see also* SFC Supp. at 7 (describing OpenLGTV projects).

[1394] LG Reply at 5.

the Librarian's consideration—LG challenges SFC's claim that circumvention would extend the lifespan of smart TVs by allowing users to add functionality that would otherwise require the purchase of a new TV. LG asserts instead that "circumvention of TPMs would only make the television more vulnerable to malware and hackers and thereby effectively decrease the life span of the product."[1395] In particular, LG argues that permitting circumvention would "compromise the overall platform security of Smart TVs," and in doing so, "place the consumer's privacy in jeopardy and expose manufacturers of Smart TVs to liability."[1396] LG urges that the TPMs "fundamentally protect the consumer's software from security risks," including by "block[ing] malware from infiltrating the television's systems."[1397] LG asserts that "circumvention of TPMs would disable the security installed in Smart TVs to prevent hackers and malware from gaining access to the user's television" such that bad actors would be able to access "a user's content and personal information."[1398]

3. Discussion

a. Noninfringing Uses

The Register concludes that proponents have carried their burden of demonstrating that circumvention of access controls on smart TV firmware is likely to enable noninfringing uses of that firmware. First, it appears to be undisputed that smart TV firmware includes a substantial number of third-party FLOSS applications, and that the licenses by which those applications are distributed expressly permit anyone to "access [them], modify their functionality, and install new or modified versions of the applications onto their TVs."[1399] In such cases, the Register concludes that the proffered uses would be licensed and thus noninfringing.

Second, with respect to non-FLOSS proprietary software applications that are part of smart TV firmware, modifications to that firmware to enable interoperability with third-party software are likely to constitute a fair use. Although SFC was rather conclusory in its fair use argument, it provided case law to support its claim that copying and alteration of computer programs to achieve interoperability can be a permissible fair use.[1400]

[1395] *Id.*

[1396] *Id.* at 4.

[1397] *Id.* at 2.

[1398] *Id.*

[1399] SFC Supp. at 5.

[1400] *See id.* at 6-7 & nn.33-34 (citing *Sega*, 977 F.2d at1528 and *Lexmark*, 387 F.3d at 550-51); SFC Reply at 5 (citing *Connectix*, 203 F.3d 596). The Register disagrees with Joint Creators's contention that SFC cannot establish fair use because it has failed to "describe[] in any detail the process of circumventing access controls." Joint Creators Class 20 Opp'n at 3. The identification of access controls is relevant to the question of whether the section 1201(a)(1) exemption process has been properly invoked, not whether the

Considering the first statutory factor for fair use, the purpose and character of the use, SFC points to a well-established line of cases supporting the conclusion that enabling interoperability with other computer programs is a favored purpose under the law, including *Sega* and *Connectix*. The Register has relied on these decisions in the past in recommending exemptions for smartphone jailbreaking.[1401] Even if the use is not considered transformative—because the firmware will still be used for its intended purpose—that is not in and of itself dispositive. As the Register concluded in 2012 in the context of granting an exemption for the jailbreaking of smartphones, even where a use is nontransformative, the first factor may nonetheless favor fair use where, as here, the purpose and character of the use is "noncommercial and personal" and the use enhances functionality.[1402] Contrary to Joint Creators' assertion, the Federal Circuit's decision in *Oracle v. Google* does not warrant a different conclusion. That case held only that interoperability concerns are not determinative of copyrightability; it expressly acknowledged that interoperability concerns "may be relevant to a fair use analysis."[1403]

Looking to the second factor, it appears indisputable that the smart TV firmware at issue is functional, rather than creative, in nature, thus weighing in favor of fair use.[1404] With regard to the third factor, the amount and substantiality of the portion taken, SFC acknowledges that jailbreaking a smart TV may require making a full copy of the firmware, including any proprietary components.[1405] This factor thus tends to weigh against fair use. But the weight afforded this factor in the overall analysis is lessened by the fact that modification of proprietary software is not always a necessity; SFC asserts, and opponents do not dispute, that installation of third-party applications may only require access to FLOSS-based firmware applications.[1406] In any event, as the Register has previously found in the smartphone context, copying of an entire computer program, when required to facilitate interoperability, does not necessarily defeat fair use.[1407]

Finally, considering the effect on the market for or value of the work, the Register agrees with SFC that "[t]here is no market for Smart TV firmware sold separately from the TVs themselves."[1408] Moreover, opponents do not explain how jailbreaking will diminish the market value of that firmware. Although LG asserts that permitting jailbreaking could "compromise the overall platform security of Smart TVs" by

---

requested use is fair. In any event, the Register finds that the access controls are sufficiently described to consider SFC's proposal.

[1401] 2010 Recommendation at 91-94.

[1402] 2012 Recommendation at 72, 74 (citing 2010 Recommendation at 93).

[1403] *Oracle v. Google*, 750 F.3d at 1376-77.

[1404] *See* SFC Supp. at 2; SFC Reply at 3 (highlighting the functional nature of the firmware by noting that it "must be compiled for the architecture of the TV it is intended to run on").

[1405] SFC Supp. at 2.

[1406] *Id.* at 5-6.

[1407] *See* 2012 Recommendation at 90, 93.

[1408] SFC Supp. at 8.

"plac[ing] the consumer's privacy in jeopardy and expos[ing] manufacturers of Smart TVs to liability,"[1409] on the current record, the Register finds these concerns to be unsubstantiated and speculative. No actual evidence was submitted to illustrate the claim that jailbreaking of smart TVs will make it easier to gain unauthorized access to copyrighted content, or that it would otherwise undermine smart TVs as a platform for the consumption of expressive works. SFC explains that access to copyrighted programming displayed or played on smart TVs from services like Hulu and Netflix "is controlled by separate TPMs" from those used to protect the smart TV firmware,[1410] and Joint Creators do not rebut this claim. Although Joint Creators express concern that jailbreaking smart TVs would permit the installation of applications that are themselves infringing—or applications such as Popcorn Time that are used to consume infringing content—once again, they do not supply actual evidence to support their claims.[1411] The Register also agrees with proponents that users who jailbreak their own smart TVs are necessarily accepting the risks that come with engaging in that activity, including the possibility of exposing themselves to malware or voiding the manufacturer's warranty. Thus, the fourth factor also favors fair use.

Accordingly, the Register concludes that proponents have met their burden of demonstrating that jailbreaking of smart TVs is likely to be a fair use.[1412]

b. Adverse Effects

Proponents have established that the prohibition on circumvention is adversely affecting legitimate noninfringing uses of smart TV firmware. In particular, SFC has provided substantial evidence that the prohibition on circumvention is preventing installation of legitimate third-party software applications that can enhance the smart TV's functionality. These applications include software to improve accessibility features for disabled users, to enable or expand the TV's compatibility with peripheral hardware and external storage devices, and to make changes to the features of the TV such as the aspect ratio.[1413]

[1409] LG Reply at 4.

[1410] SFC Supp. at 10.

[1411] The Register notes that if such a correlation were to be demonstrated in a future proceeding, it could impact the Register's analysis. In the case of video game consoles, for example—where opponents have shown that jailbreaking of consoles is strongly associated with the consumption of unauthorized content—the Register has declined to grant a jailbreaking exemption. *See* 2012 Recommendation at 42-44.

[1412] Although no opponent opposed SFC's invocation of section 117 as another potential basis for noninfringing use, the burden is on the proponent to establish entitlement to the exemption. NOI, 79 Fed. Reg. at 55,689. SFC fails to carry that burden here, because it provided no evidence or argument to demonstrate that the owner of a smart TV owns, rather than licenses, the proprietary applications incorporated into a smart TVs firmware. 17 U.S.C. § 117(a)(1) (extending the limitation to "the owner of a copy of a computer program"); *see also Krause v. Titleserv, Inc.*, 402 F.3d 119, 122 (2d Cir. 2005); *Vernor v. Autodesk, Inc.*, 621 F.3d 1102, 1111-12 (9th Cir. 2010).

[1413] SFC Supp. at 5-6.

Even assuming LG is correct that its smart TVs already provide some or all of these capabilities, SFC testified that the same is not true of all smart TVs.[1414] Furthermore, the Register rejects Joint Creators' suggestion that connecting a laptop to a TV serves as a viable alternative to circumvention. That solution would only provide access to applications and content accessible from the laptop. It would not allow installation of software on the smart TV to improve its functioning as a TV, such as making changes to permit better interoperability of the TV with accessibility devices or facilitating more prominent subtitles.

c. Statutory Factors

Under the first statutory factor, the availability for use of copyrighted works, the record indicates that third-party applications exist to improve the functionality of smart TVs.[1415] Similar to past determinations reached with respect to jailbreaking of smartphones, the Register concludes that the access controls at issue prevent consumers from using these third-party applications, and that denying a jailbreaking exemption for smart TVs would diminish the availability of such works.[1416] At the same time, as explained above, there is no evidence that granting the exemption would diminish the availability of manufacturer-installed smart TV firmware.

The Register concludes that factor two, concerning the availability of works for nonprofit archival, preservation, and educational uses, marginally favors granting the exemption. SFC credibly asserts that one of the primary purposes of the FLOSS licenses is to allow users to study and learn from the FLOSS applications they use and that the exemption here will further that purpose.[1417] With respect to factor three, the impact on criticism, comment, news reporting, teaching, scholarship, or research, while the Register acknowledges SFC's observation that jailbreaking might enable some types of security research, such activities are not the focus of the proposal.[1418] Factor three is therefore neutral.

Under the fourth factor, concerning the "effect of circumvention of technological measures on the market for or value of the copyrighted works,"[1419] as noted above in the fair use analysis, there is no evidence in the current record that jailbreaking smart TVs will harm the market for smart TV firmware or for other expressive works. Under the fifth statutory factor, SFC asserts that the exemption would extend the lifespan of smart

[1414] Tr. at 132:10-133:08 (May 20, 2015) (Williamson, SFC).

[1415] *See* SFC Supp. at 5-6 (citing SamyGO project).

[1416] *See* 2012 Recommendation at 76 (citing 2010 Recommendation at 101).

[1417] SFC Supp. at 8.

[1418] *Id.* at 8-9; Tr. at 143:03-19 (May 20, 2015) (noting the potential for serious security vulnerabilities in smart TV software). Circumvention for purposes of security research is considered in Proposed Classes 22, 25, and 27A.

[1419] 17 U.S.C. § 1201(a)(1)(C)(iv).

TVs by allowing users to add new functionality to them,[1420] while LG argues that the exemption would shorten the lifespan of smart TVs by making them more vulnerable to malware.[1421] As neither of these competing claims is adequately substantiated, the Register concludes that the fifth factor is neutral.

In sum, on the whole, the statutory factors support the granting of an exemption.

4. NTIA Comments

NTIA supports an exemption to allow circumvention of access controls on smart TV firmware for purposes of enabling interoperability with third-party applications.[1422] In NTIA's view, the proposed exemption "does not raise significantly different issues than those the Register has previously considered regarding the jailbreaking of mobile phones."[1423] NTIA notes in particular that "there are accessibility needs that cannot always be met without circumvention, such as modifying subtitles to enhance readability or changing the aspect ratio or resolution of the television."[1424]

5. Conclusion and Recommendation

For the reasons described above, proponents of Class 20 have satisfied their burden of showing that TPMs applied to smart TVs have an adverse effect on noninfringing uses. The statutory factors also tip in favor of granting the exemption.

Accordingly, the Register recommends that the Librarian designate the following class:

> **Computer programs that enable smart televisions 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 smart television.**

[1420] SFC Supp. at 10.

[1421] LG Reply at 5.

[1422] NTIA Letter at 52.

[1423] *Id.* at 50.

[1424] *Id.*

I. Proposed Class 21: Vehicle Software – Diagnosis, Repair or Modification

1. Proposals

Modern automobiles and agricultural vehicles and machinery are equipped with systems of interconnected computers that monitor and control a variety of vehicle functions.[1425] As modern vehicles have become more reliant on software to operate, a wide variety of diagnostic, repair and modification activities now require access to and sometimes alteration of those computer programs, including identifying malfunctions, installing replacement parts, and customizing vehicles for specialized uses.[1426] As is explained below, however, manufacturers restrict access to vehicle computer programs in a variety of ways. Accordingly, proponents are requesting an exemption to permit circumvention of TPMs protecting computer programs[1427] that control the functioning of vehicles for the purposes of diagnosis, repair and modification of the vehicles.

EFF filed a petition seeking an exemption to allow the circumvention of TPMs on computer programs that are embedded in vehicles for purposes of personalization, modification, or other improvement of the vehicle. The exemption would apply to all motorized land vehicles.[1428]

IPTC USC proposed two similar exemptions for agricultural machinery specifically.[1429] The proposed exemptions would allow owners of agricultural vehicles to circumvent the TPMs on computer programs that are embedded in their vehicles for the purpose of modifying, and to diagnose and/or repair, those vehicles.

These proposals were consolidated by the Office into a single proposed class, described as follows in the NPRM:

[1425] The Electronic Frontier Foundation ("EFF") Vehicle Software Repair Pet. at 2.

[1426] *Id.* ; The Intellectual Property & Technology Law Clinic of the University of Southern California Gould School of Law ("IPTC USC") Vehicle Software Modification Pet. at 1, 4; IPTC USC Vehicle Software Repair Pet. at 1, 4.

[1427] The Register notes that throughout this Recommendation, the terms "firmware" and "software" are variously used, although both are "computer programs" within the meaning of the Copyright Act. *See* 17 U.S.C. § 101 (definition of "computer program").

[1428] EFF's proposed regulatory language reads as follows: "Lawfully-obtained computer programs that control or are intended to control the functioning of a motorized land vehicle, including firmware and firmware updates, where circumvention is undertaken by or on behalf of the lawful owner of such a vehicle for the purpose of lawful aftermarket personalization, improvement, or repair." EFF Vehicle Software Repair Pet. at 1.

[1429] IPTC USC filed two petitions relating to agricultural machinery software. The first seeks an exemption to "allow[] farmers to circumvent . . . TPMs for the purpose of modifying their own agricultural machinery to improve efficiency and/or functionality." IPTC USC Vehicle Software Modification Pet. at 1. The second seeks an exemption to "allow[] farmers to circumvent . . . TPMs for the purpose of diagnosing and/or repairing their own agricultural machinery." IPTC USC Vehicle Software Repair Pet. at 1.

> Proposed Class 21: This proposed class would allow circumvention of TPMs protecting computer programs that control the functioning of a motorized land vehicle, including personal automobiles, commercial motor vehicles, and agricultural machinery, for purposes of lawful diagnosis and repair, or aftermarket personalization, modification, or other improvement. Under the exemption as proposed, circumvention would be allowed when undertaken by or on behalf of the lawful owner of the vehicle.[1430]

In addition to EFF and IPTC USC, the Office received comments supporting the proposed exemption from AAA,[1431] Auto Care Association and Automotive Parts Remanufacturers Association ("Auto Care"),[1432] Catherine Gellis and the Digital Age Defense project ("Gellis/Digital Age Defense"),[1433] Consumer Electronics Association ("CEA"),[1434] Farm Hack,[1435] Free Software Foundation ("FSF"),[1436] iFixit,[1437] National Corn Growers Association,[1438] Randy's Repair, LLC.,[1439] Specialty Equipment Market Association ("SEMA"),[1440] and over 2500 individuals.[1441] Two parties, SAE International Dedicated Short Range Communication Standards Committee ("SAE DSRC") and SAE Vehicle Electrical System Security (VESS) Committee ("SAE VESS"), submitted neutral comments, along with offers to assist the Copyright Office by providing and sharing their technical expertise.[1442]

a. Background

As noted above, modern vehicles are equipped with computers that monitor and control vehicle functions. These computers are referred to as electronic control units, or

[1430] NPRM, 79 Fed. Reg. at 73,869. In discussing this class, the Register uses the term "vehicle" to refer generally to all the types of motorized vehicles listed in the proposed exemption language, including agricultural machinery.

[1431] AAA Reply.

[1432] Auto Care Reply.

[1433] Gellis/Digital Age Defense Class 21 Supp.

[1434] CEA Reply.

[1435] Farm Hack Supp.

[1436] FSF Class 21 Supp.

[1437] iFixit & Kyle Wiens Supp.; iFixit Class 21 Supp.; iFixit Reply.

[1438] National Corn Growers Association Reply.

[1439] Randy's Repair, LLC. Reply.

[1440] SEMA Reply.

[1441] Digital Right to Repair Class 21 Supp. (2284 individuals); Jay Freeman Class 21 Supp.; Scott Rogers Supp.; Digital Right to Repair Class 21 Reply (298 individuals); DANNiE D Reply; David M. Lawrence Reply; David Ricotta Reply; Donna Eno Class 21 Reply; Drayton Green Reply; Edward Brown Reply; George Cothran Reply; George Sawyer Class 21 Reply; Louis Wesler Class 21 Reply; Perry Bruns Reply.

[1442] SAE DSRC Class 21 Supp.; SAE VESS Class 21 Reply.

ECUs.[1443] A vehicle may have several ECUs that facilitate its operation. The individual ECUs are programmed to fulfill specific vehicular functions, such as engine control, fuel efficiency and braking.[1444] There are several types of TPMs that restrict access to the software programs contained in ECUs, including challenge-response mechanisms, encryption, and disabled access ports on the circuitry itself.[1445]

EFF explains that while vehicle owners expect to be able to engage in diagnosis, repair, and modification activities, TPMs on vehicle software "block such legitimate activities, forcing vehicle owners to choose between breaking the law or tinkering [with] and repairing their vehicles."[1446] IPTC USC similarly notes that farmers specifically require access to vehicle software "to make any significant modifications to the efficiency and/or functionality of . . . their increasingly sophisticated agricultural machinery"[1447] and to "obtain vital diagnostic information."[1448]

b. Asserted Noninfringing Uses

Citing the four-factor fair use test set forth in section 107, Class 21 proponents assert that vehicle owners, independent mechanics, and third-party innovators are entitled to use the computer programs in ECUs to diagnose, repair, or modify vehicles as a matter of fair use. They further assert that these activities are noninfringing pursuant to the statutory exception for computer programs embodied in section 117, which exempts certain uses of computer programs from infringement liability. The Register reviews each theory of noninfringing use in turn.

i. Fair Use

On the question of fair use, addressing the first statutory factor, proponents maintain that accessing and using copyright-protected ECU computer programs to diagnose, repair and modify vehicles serve transformative purposes.[1449] Proponents assert that if the exemption were to be granted, users would be empowered to dissect and understand the functional aspects of these programs in order to create tools and applications for use on or in coordination with ECUs.[1450] In the case of modification, proponents maintain that the exemption would allow the addition of new functions and enhancement of existing functions to suit users' particular needs, as well as necessary

[1443] EFF Vehicle Software Repair Pet. at 2; IPTC USC Vehicle Software Modification Pet. at 1; IPTC USC Vehicle Software Repair Pet. at 1.

[1444] EFF Vehicle Software Repair Pet. at 1; IPTC USC Vehicle Software Modification Pet. at 4.

[1445] *See, e.g.*, EFF Class 21 Supp. at 3-4; IPTC USC Class 21 Supp. at 5-6.

[1446] EFF Vehicle Software Repair Pet. at 5.

[1447] IPTC USC Vehicle Software Modification Pet. at 1.

[1448] IPTC USC Vehicle Software Repair Pet. at 1.

[1449] EFF Class 21 Supp. at 8-9 (citing *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 579 (1994)).

[1450] *Id.* at 8; *see also* EFF Class 21 Reply at 4-7; IPTC USC Class 21 Supp. at 11-12; IPTC USC Class 21 Reply at 8-9.

modifications to ECUs to accommodate replacement parts. They urge that these uses are transformative, and that this conclusion alone requires a finding of fair use.[1451]

Turning to the second fair use factor, proponents state that the nature of the computer programs on ECUs weighs heavily in favor of fair use because the programs contain "unprotected aspects that cannot be examined without copying."[1452] They also note that the computer programs at issue act much like an internal operating system and thus lie "'at a distance from the core' of copyright protection."[1453] In particular, proponents observe that in prior 1201 rulemaking proceedings, the Register had concluded that computer programs comprising bootloaders and operating systems are essentially functional and that "[a]s functional works, certain features are dictated by function and in order to interoperate with [other] works certain functional elements of those programs, elements that in and of themselves may or may not be copyrightable, must be modified."[1454] Proponents thus urge that "where the nature of the work is such that purely functional elements exist in the work and it is necessary to copy the expressive elements in order to perform those functions, consideration of this second factor arguably supports a finding that the use is fair."[1455]

With regard to the third factor, the amount of the copyrighted work used, proponents recognize that the entire work may be used. However, they note that this does not preclude a finding of fair use. They observe that the relevant analysis includes a consideration of whether the quantity and value of the materials used are reasonable in relation to the purpose of the copying.[1456] They reiterate that because it is necessary to copy the entire work in order to achieve a transformative purpose, consideration of this third factor arguably supports a finding that the use is fair.[1457] They assert that in the case of the diagnosis, repair, or modification of vehicle functions, any reproduction or alteration of computer programs on ECUs will only be that which is reasonable and for a legitimate purpose.[1458]

[1451] *See, e.g.*, EFF Class 21 Supp. at 7-11; EFF Class 21 Reply at 4-8; IPTC USC Class 21 Supp. at 11-12; IPTC USC Class 21 Reply at 8-10.

[1452] *See, e.g.*, IPTC USC Class 21 Supp. at 12 (quoting *Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596, 603 (9th Cir. 2000)).

[1453] See, *e.g.*, *id.*

[1454] EFF Class 21 Supp. at 9 (quoting 2010 Recommendation at 96); Auto Care Class 21 Reply at 8 (same).

[1455] EFF Class 21 Supp. at 9 (quoting *Oracle Am., Inc. v. Google Inc.*, 750 F.3d 1339, 1375 (Fed. Cir. 2014)).

[1456] *Id.* at 10 (citing *Campbell*, 510 U.S. at 586-87); IPTC USC Class 21 Supp. at 11 (citing *Perfect 10, Inc. v. Amazon, Inc.*, 508 F.3d 1146, 1165 (9th Cir. 2007)).

[1457] IPTC USC Class 21 Reply at 9 (citing *Authors Guild, Inc. v. HathiTrust*, 755 F.3d 87, 98 (2d Cir. 2014)).

[1458] EFF Class 21 Supp. at 10; EFF Class 21 Reply at 7-8.

Finally, proponents assert that the fourth factor, the effect on the market for or value of the copyrighted work, also favors fair use.[1459] Proponents note that there is no market for computer programs on ECUs apart from the sale of vehicles themselves, and so the uses encompassed by the proposed exemption, by definition, cannot substitute for sales of the vehicle software.[1460] Proponents also maintain that the relevant market for consideration is the market for the copyrighted works themselves and not the market for vehicles containing the ECUs.[1461] Accordingly, proponents reject as inapposite opponents' claims regarding market effects such as vehicle values and brand equity.[1462]

ii. Section 117

Proponents also assert that vehicle owners' copying or alteration of computer programs for diagnosis, repair or modification purposes on ECUs is noninfringing under section 117. That provision allows the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that program "as an essential step in the utilization of the computer program in conjunction with a machine and [if] it is used in no other manner."[1463]

A key consideration with respect to the application of section 117 is who owns the computer program in question. Proponents argue that under either of the two leading tests for ownership under section 117—*Krause v. Titleserv, Inc.*[1464] and *Vernor v. Autodesk, Inc.*[1465]—it is the owners of the vehicles who own the copies of the programs on ECUs embedded within those vehicles.[1466] Proponents state that most vehicle ECUs are transferred with the vehicle with no explicit agreements governing title to the copies of ECU computer programs.[1467] Proponents explained during the initial round of comments that they were able to identify only a few license agreements pertaining to ECUs. These agreements addressed only specific telematics[1468] or entertainment systems; proponents did not locate any licenses covering more general vehicle

[1459] *See, e.g.*, EFF Class 21 Supp. at 11; EFF Class 21 Reply at 8; IPTC USC Class 21 Supp. at 12; IPTC USC Class 21 Reply at 10.

[1460] EFF Class 21 Supp. at 11; IPTC USC Class 21 Supp. at 12.

[1461] IPTC USC Class 21 Reply at 10.

[1462] EFF Class 21 Reply at 8; IPTC USC Class 21 Reply at 10.

[1463] 17 U.S.C. § 117(a)(1).

[1464] 402 F.3d 119 (2d Cir. 2005).

[1465] 621 F.3d 1102 (9th Cir. 2010).

[1466] *See, e.g.*, EFF Class 21 Supp. at 11-15; EFF Class 21 Reply at 9-12; IPTC USC Class 21 Reply at 4-5.

[1467] EFF Class 21 Supp. at 13; *see also* Tr. at 183:02-12 (May 19, 2015) (Walsh, EFF).

[1468] EFF Class 21 Supp. at 14 (citing *Terms and Conditions of Your Safety Connect Telematics Service*, TOYOTA 4 (Oct. 20, 2010), http://www.toyota.com/safety-connect/img/safetyconnect-terms.pdf (establishing that telematics systems are vehicle systems that combine global positioning satellite tracking and other wireless communications to identify the location of vehicles for a variety of purposes such as automatic roadside assistance)).

functions.[1469] And, during the reply phase, proponents noted that opponents had failed to offer any further evidence that copies of computer programs on ECUs are licensed rather than sold to vehicle purchasers.[1470]

Proponents further maintain that even if written license terms exist, a vehicle owner can nonetheless be considered the owner of the ECU software copies. They note that possessing actual title to a copy of a work is not an "absolute prerequisite" to section 117(a) protection.[1471] Rather, a party who exercises sufficient incidents of ownership over a copy of the program can be considered the owner of it.[1472] They assert that such incidents of ownership exist for vehicle purchasers, noting that vehicle owners are understood to have the right to indefinitely use, possess, resell, discard or destroy their vehicles, including the embedded ECUs, without any material restriction from the manufacturer, and that no opponent has introduced any contrary evidence.[1473] Proponents rely as well on the Register's conclusion, in the context of granting an exemption for cellphone "unlocking," that under applicable precedent, at least some subset of cellphone owners may be considered to own the copy of the cellphone software on their devices.[1474]

Proponents additionally assert that making copies or adaptations of ECU computer programs for the desired uses is "an essential step in the utilization of the computer program in conjunction with a machine and that [the copy or adaptation] is used in no other manner," as required to invoke section 117.[1475] Although proponents concede that making such copies and adaptations may not be essential to using the vehicle in the manner intended by the manufacturer, they stress that section 117 allows the making of such copies and adaptations for the purpose of adding new features and capabilities to that software, noting that *Krause* had "approved the modifications and deemed them essential not because they were necessary to make the software *work*, but because they were necessary to make the software *helpful* or worth using."[1476] Additionally, proponents maintain that the creation of a backup copy to protect against destruction of or damage to the ECU software in the process of diagnosis, repair or

[1469] *Id.* at 13-14 (citing end-user license agreements for GM OnStar, Pioneer AppRadioLIVE, Ford Sync, Toyota Safety Connect, and Mercedes-Benz mbrace).

[1470] EFF Class 21 Reply at 9; IPTC USC Class 21 Reply at 4-5.

[1471] IPTC USC Class 21 Reply at 4 (citing *Krause*, 402 F.3d at 124).

[1472] *Id.*

[1473] *Id.* at 4-5; EFF Class 21 Reply at 9-10.

[1474] IPTC USC Class 21 Reply at 7 (citing 2012 Recommendation at 92-93).

[1475] *See, e.g.*, EFF Class 21 Supp. at 13 (quoting 17 U.S.C. § 117(a)(1)).

[1476] *Id.* at 15 (internal quotation marks omitted) (citing *Softech Worldwide, LLC v. Internet Tech. Broad. Corp.*, 761 F. Supp. 2d 367, 373 & n.2 (E.D. Va. 2011) (describing *Krause*)); *see also Krause*, 402 F.3d at 126-27 (holding that section 117 encompassed "changes [that] were not strictly necessary to keep the programs functioning, but were designed to improve their functionality in serving the business for which they were created").

modification is covered by the archival purposes exception set forth in section 117(a)(2).[1477]

c. Asserted Adverse Effects

Proponents maintain that vehicle owners expect to have the freedom to diagnose, repair, or modify their own vehicles, and that access to the computer programs in the ECUs is required for these purposes.[1478] They cite numerous examples of diagnosis, repair and/or modification activities in which vehicle owners have traditionally engaged—such as performance of routine maintenance, including oil changes,[1479] resetting service warning lights,[1480] fixing safety items like seatbelts,[1481] and enhancing suspensions[1482]—that would, or would likely be, impeded by the prohibition on circumvention today. Moreover, EFF explains that "it is common for repairs that replace hardware components to require modifications [of ECU programs] in order to calibrate the new part," explaining, for example, that "[i]f new gears have a different radius than old ones, the computer needs to know so that the speedometer will work correctly."[1483]

Proponents claim, however, that because of the existence of TPMs on vehicle software, vehicle owners must take their cars to authorized repair shops, or purchase expensive manufacturer-authorized tools, to diagnose and repair their vehicles.[1484] They also suggest that in some instances, TPMs prevent vehicle owners from making lawful modifications to their vehicles, such as modifying the car "to cap the speed when they lend the car to their teenage children or to a valet."[1485] Moreover, proponents allege that manufacturer-licensed tools may not always allow a user to diagnose and repair a problem.[1486] For instance, Craig Smith of Open Garages gave the example of a colleague who attempted to diagnose an inoperable power window on a car, where the authorized diagnostic tool indicated the window was operational. Smith explained that through

[1477] *See, e.g.*, EFF Class 21 Reply at 11-12.

[1478] *See, e.g.*, EFF Class 21 Supp. at 16-23; EFF Class 21 Reply at 12-20; IPTC USC Class 21 Supp. at 12-18; IPTC USC Class 21 Reply at 10-11.

[1479] EFF Class 21 Supp. at 18.

[1480] *Id.*

[1481] IPTC USC Class 21 Supp. at 14.

[1482] *Id.* at 10.

[1483] EFF Class 21 Supp. at 7; *see also id.* at App. A at 1-2 (Statement of David Blundell) (highlighting modifications that require reprogramming of ECUs, including installing "a different rear axle gear . . . to improve its ability to tow heavy loads" and to accommodate changes in tire size).

[1484] *Id.* at 17-19; IPTC USC Class 21 Supp. at 14-15.

[1485] EFF Class 21 Supp. at 20-21; *see also* IPTC USC Supp. at 16-17 (explaining that manufacturers of agricultural equipment "tend to program ECUs to completely shut the machine down if they detect aftermarket 'modules' which users can attach to modify performance characteristics").

[1486] Tr. at 223:22-224:10 (May 19, 2015) (Charlesworth, USCO; Smith, Open Garages).

reverse engineering the vehicle software, he and his colleague were able to determine that the communications system for the power window unit was faulty.[1487]

IPTC USC maintains that TPMs restricting access to agricultural vehicles and machinery place the livelihoods of farmers and other business owners at risk, because vehicle owners must sometimes wait significant periods of time before their disabled vehicles can be repaired by an authorized technician.[1488] Proponents further assert that TPMs force vehicle owners to pay higher prices to authorized repair shops; prevent them from using their local, chosen and/or trusted service providers; reduce competition in the repair market by allowing manufacturers to monopolize diagnosis and repair of vehicles; cause vehicle owners to delay repairs, sometimes at a cost to user comfort, ease or safety; prevent vehicle owners from safely increasing engine power; prevent vehicle owners from increasing environmental efficiency; prevent vehicle owners with disabilities from enhancing accessibility; and distort secondary markets for vehicles.[1489] Proponents assert that as vehicles are embedded with greater capabilities, such as self-driving functions, that are controlled by TPM-protected ECUs, the negative effects will only increase.[1490]

Proponents also challenge opponents' claim that alternatives to circumvention mitigate the adverse impact of TPMs. As explained in greater detail below, opponents assert that a 2014 nationwide memorandum of understanding ("MOU"),[1491] entered into by auto manufacturers, aftermarket parts manufacturers, and independent repair shops, broadly authorizes diagnosis and repair activities without the need for circumvention.[1492] Proponents, however, argue that this industry arrangement is too narrow to mitigate the adverse impact of TPMs on vehicle owners.[1493] For instance, proponents note that the MOU regime leaves out many vehicles: the MOU encompasses only certain model years;[1494] not all manufacturers of automobiles are party to the MOU;[1495] and certain types of vehicles, such as mechanized agricultural vehicles, motorcycles and RVs, are not

[1487] *See id.* at 222:09-20 (Smith, Open Garages). Note that the transcript for the hearing refers to the window unit's "cannibus." This is a typo, and should instead read "CAN bus," which is the network by which vehicle ECUs communicate with each other. *See* John Deere Class 21 Opp'n at 23; Tr. at 15:12-21 (May 19, 2015) (Miller).

[1488] IPTC USC Class 21 Supp. at 12-13 ("Without an exemption, farmers must often send their machines to far-away dealerships, or wait for a technician to travel to their farm to perform diagnostics and repairs—even for minor problems such as a blown fuse.").

[1489] *See, e.g.*, EFF Class 21 Supp. at 16-23; EFF Class 21 Reply at 12-20; IPTC USC Class 21 Supp. at 12-18; IPTC USC Class 21 Reply at 10-11.

[1490] *See, e.g.*, EFF Class 21 Supp. at 16-17.

[1491] *See* Auto Alliance Class 21 Opp'n at Exhibit A.

[1492] *See id.* at 12-16.

[1493] *See, e.g.*, EFF Class 21 Reply at 17-18; IPTC USC Class 21 Reply at 11-12.

[1494] EFF Class 21 Reply at 17 ("The MoU excludes roughly half of motorized land vehicles now operating in the United States."); *see also id*. (noting that certain obligations of the MOU need not be implemented until January 2, 2019, "*after* the three-year period covered by this rulemaking").

[1495] IPTC USC Class 21 Reply at 12; EFF Class 21 Reply at 17.

covered by the MOU.[1496] In addition, proponents observe that the MOU focuses on enabling diagnosis and repair, but does not generally enable vehicle owners to engage in vehicle modification.[1497]

d. Argument Under Statutory Factors

Proponents maintain that the statutory factors set forth in section 1201(a)(1) support their request. Concerning the first statutory factor, Class 21 proponents argue that the availability of copyrighted works will not be harmed by granting the exemption.[1498] They assert that the exemption will not "diminish the[] production of vehicle software."[1499] Proponents also maintain that the proposed exemption will increase access to copyrighted works, because the computer programs on ECUs currently in the marketplace are not available for vehicle owners to "'use' in the copyright sense of conduct that implicates the rights enumerated in Section 106."[1500] Proponents also believe that the information made accessible via the proposed exemption will lead to the creation of additional copyrighted works that explain the operation of car software, such as the *Car Hacker's Handbook*, an online manual that provides information about vehicle computer systems.[1501]

Regarding the second factor, the availability for use of works for nonprofit archival, preservation, and educational purposes, proponent IPTC USC concedes that it is unaware of "any potential uses that would fall under this factor."[1502] EFF, however, maintains that the proposed exemption will increase public knowledge of the computer programs in ECUs by allowing vehicle owners to participate in educational activities, such as tinkering and exchanging information about those programs.[1503] Additionally, EFF asserts that the exemption would facilitate archival use of computer programs on ECUs, in the form of software backups, which they describe as a routine and advisable step in the process of lawful diagnosis and repair, or modification.[1504]

[1496] *See, e.g.*, EFF Class 21 Reply at 17; IPTC USC Class 21 Reply at 12; *see also* Tr. at 228:25-229:01 (May 19, 2015) (Lightsey, GM).

[1497] *See, e.g.*, IPTC USC Class 21 Reply at 12.

[1498] EFF Class 21 Supp. at 23.

[1499] EFF Class 21 Reply at 20.

[1500] *Id.*

[1501] *See* EFF Class 21 Supp. at 23 ("Craig Smith, author of the *2014 Car Hacker's Handbook*, reported that the Handbook was downloaded 300,000 times in the first two weeks it was available."). The *Car Hacker's Handbook* offers information about how to analyze the computer systems inside vehicles and determine whether there are security weaknesses. Craig Smith, 2014 CAR HACKER'S HANDBOOK (2014), *available at* http://opengarages.org/handbook.

[1502] *See* IPTC USC Class 24 Supp. at 19-20 ("We have not investigated any potential uses that would fall under this factor.").

[1503] EFF Class 21 Supp. at 23-24.

[1504] *See, e.g.*, EFF Class 21 Reply at 11-12.

With respect to the third factor, the impact that the prohibition on circumvention has on criticism, comment, news reporting, teaching, scholarship or research, while some proponents fail to offer any evidence on this point,[1505] EFF maintains that vehicle owners' fear of incurring liability under section 1201(a)(1)'s prohibition on circumvention negatively impacts speech in relation to each of the activities listed under this factor.[1506] It also argues that an exemption would enhance the ability to produce new copyrighted works, such as the *Car Hacker's Handbook*.[1507]

Regarding factor four, the effect of circumvention on the market for or value of copyrighted works, proponents argue that the market value of computer programs used in ECUs would not be harmed by the proposed exemption at all. Proponents urge that because "the copyrighted work is sold to end-users along with an entire vehicle," simply allowing users to access or modify the copy of the work in their own vehicle has no effect on the market for the software.[1508] Proponents further assert that the proposed exemption will not negatively impact the sales or production of computer programs used in ECUs, because auto manufacturers will still be able to sell vehicles at "substantially the same price," and the exemption will primarily drive the development of aftermarket software products.[1509]

Proponents offered little input on the fifth statutory factor, which concerns such other factors as the Librarian considers appropriate. As discussed below, however, opponents rely heavily on this provision to raise potential public safety, security, and environmental concerns with respect to the proposed exemption. Proponents respond by urging that such concerns are purely speculative and, in any event, unrelated to the copyright concerns that underlie section 1201.[1510] They maintain that these concerns are better addressed via laws designed specifically for those purposes, rather than being swept up in the blanket prohibition embodied in section 1201.[1511] Moreover, in response to the specific concern about whether purchasers of used vehicles would be able to detect whether a previous owner had made changes to the ECU, EFF argued that it would be possible to detect such changes.[1512]

[1505] *See, e.g.*, IPTC USC Class 21 Supp. at 20.

[1506] EFF Class 21 Supp. at 24 ("The legal cloud resulting from the prohibition on circumvention reduces participation in research, scholarship and teaching on vehicle functionality, repair, and modification, as well as critiquing, commenting, and reporting on the functionality of manufacturer software and potential alternatives.").

[1507] *Id.* at 23-24.

[1508] *Id.* at 11, 25.

[1509] IPTC USC Class 21 Supp. at 20.

[1510] IPTC USC Class 21 Reply at 14.

[1511] *See, e.g., id.* at 14-15; EFF Class 21 Reply at 18-21; Tr. at 189:24-190:14 (May 19, 2015) (Walsh, EFF).

[1512] EFF Class 21 Post-Hearing Resp. at 2-4.

2. Opposition

The Office received comments in opposition to the proposed exemption from Association of Equipment Manufacturers ("AEM"), Association of Global Automakers ("Global Automakers"), Alliance of Automobile Manufacturers ("Auto Alliance"), Eaton Corporation, General Motors ("GM"), John Deere, and Motor & Equipment Manufacturers Association ("MEMA").[1513]

a. Asserted Noninfringing Uses

Opponents challenge the view that the diagnosis, repair, or modification activities that would be covered by the Class 21 exemption qualify as noninfringing.[1514]

Opponents first dispute the claim that the proposed activities are fair uses under section 107.[1515] Under the first fair use factor, opponents argue that consideration of the purpose and character of the use weighs against a fair use finding.[1516] Several opponents contend that proponents' proposed uses would require accessing and altering computer programs on ECUs so that they perform the identical function as they previously did, albeit with different parameters or values, and that such uses are not transformative.[1517] GM also notes that the exemption is not limited to allowing the creation of interoperable tools.[1518] John Deere, meanwhile, contends that the exemption would allow proponents to modify ECUs to undermine or reverse the purposes for which the computer programs were intended by enabling and encouraging noncompliance with environmental regulations and that such a use is of a purpose and character that should be disfavored under section 107.[1519] And, while Global Automakers concedes that the exempted activity would involve altering automotive functions, it maintains that such use is not the sort of transformative use that is contemplated by the first fair use factor.[1520]

[1513] AEM Opp'n; Global Automakers Class 21 Opp'n; Auto Alliance Class 21 Opp'n; Eaton Corp. Opp'n; GM Class 21 Opp'n; John Deere Class 21 Opp'n; MEMA Class 21 Reply. The Register notes that MEMA filed its comments in the reply phase of the written comment period, which had been designated as allowing proponents and neutral commenters to respond to points made by the opposition. The Register will exercise her discretion to consider MEMA's comments in reply, while at the same time being mindful that proponents did not have an opportunity to file written comments in response to MEMA.

[1514] *See, e.g.*, Auto Alliance Class 21 Opp'n at 4-11; John Deere Class 21 Opp'n at 4-9.

[1515] *See, e.g.*, Global Automakers Class 21 Opp'n at 4-5; Auto Alliance Class 21 Opp'n at 8-11; GM Class 21 Opp'n at 14-18; John Deere Class 21 Opp'n at 6-9.

[1516] *See, e.g.*, Global Automakers Class 21 Opp'n at 4-5; Auto Alliance Class 21 Opp'n at 7-8; GM Class 21 Opp'n at 14-16; John Deere Class 21 Opp'n at 6-7.

[1517] GM Class 21 Opp'n at 14-16; Auto Alliance Class 21 Opp'n at 8.

[1518] GM Class 21 Opp'n at 14-15; Auto Alliance Class 21 Opp'n at 8.

[1519] John Deere Class 21 Opp'n at 6-7.

[1520] Global Automakers Class 21 Opp'n at 4.

In opponents' view, the second fair use factor, the nature of the copyrighted work, also favors a finding that the proposed uses do not qualify as fair use.[1521] John Deere and Auto Alliance recognize that ECU software is functional in nature.[1522] Additionally, they note that the Register has previously concluded that computer programs used to operate devices like smartphones are functional works.[1523] Nonetheless, John Deere and Auto Alliance urge that the Register should reconsider this position, or at least distinguish between the computer programs on ECUs and those on the smartphones in prior rulemakings.[1524] For its part, GM asserts that the computer programs at issue are "highly creative" and "expressive," noting the time and resources devoted to their development.[1525] It urges that while elements of such programs are functional, the works are nonetheless deserving of protection.[1526]

With respect to the third fair use factor, directed to the amount and substantiality of the portion used, opponents uniformly maintain that the proposed uses require copying the bulk, if not the entirety, of the copyrighted work.[1527] Additionally, they observe that the essence or essential part of the work will remain in the modified copy.[1528] Therefore, they urge that the third factor strongly indicates that the proposed uses are not fair.[1529]

Turning to the fourth factor, regarding the impact on the market for or value of the work, Auto Alliance admits that there is no separate market for the computer programs at issue aside from the market for the vehicle in which they are embedded.[1530] Auto Alliance and other opponents nonetheless maintain that vehicle values may be adversely affected indirectly.[1531] Opponents argue that if the exemption is granted, vehicles are likely to become out of compliance with regulatory standards in areas such as fuel economy, emissions control, and safety, which could negatively impact the ability to resell a car, or a subsequent purchaser's ability to meet state registration requirements.[1532]

[1521] *See, e.g.*, Auto Alliance Class 21 Opp'n at 8; John Deere Class 21 Opp'n at 7-8; GM Class 21 Opp'n at 16; Global Automakers Class 21 Opp'n at 5.

[1522] Auto Alliance Class 21 Opp'n at 8; John Deere Class 21 Opp'n at 7-8.

[1523] *Id.*

[1524] Auto Alliance Class 21 Opp'n at 8 (citing 2012 Recommendation at 73); John Deere Class 21 Opp'n at 7-8.

[1525] GM Class 21 Opp'n at 16.

[1526] *Id.*

[1527] *See, e.g.*, Auto Alliance Class 21 Opp'n at 9; John Deere Class 21 Opp'n at 8; GM Class 21 Opp'n at 17; Global Automakers Class 21 Opp'n at 5.

[1528] *See, e.g., id.*

[1529] *See, e.g.*, Auto Alliance Class 21 Opp'n at 9; John Deere Class 21 Opp'n at 9; GM Class 21 Opp'n at 17; Global Automakers Class 21 Opp'n at 5.

[1530] Auto Alliance Class 21 Opp'n at 9.

[1531] *See, e.g., id.* at 9-10; John Deere Class 21 Opp'n at 9; GM Class 21 Opp'n at 17-18; Global Automakers Class 21 Opp'n at 5.

John Deere also asserts that the activity covered under the exemption could erode the public's trust in the safety and security of vehicles, thereby diminishing demand for new vehicles.[1533]

In addition, opponents assert that the proposed uses do not fall within section 117.[1534] Opponents suggest that proponents have failed to demonstrate that vehicle owners are the owners of the computer programs on ECUs or that the broad set of uses covered by the proposed exemption all fall within the narrow exceptions specified in section 117.[1535] They note that proponents cite the same two cases considered in the 2012 Recommendation, *Krause* and *Vernor*, in which the Register observed the uncertain state of the law regarding ownership of software.[1536] Relying chiefly on the license agreements for entertainment and telematics software identified by proponents in their opening comments, opponents assert that proponents have failed to demonstrate that vehicle owners own the software that controls the vehicle ECUs under the test set forth in either case.[1537] However, opponents conceded at the public hearing that there were no written license agreements covering other types of ECUs in automobiles.[1538] Neither opponents nor proponents offered any evidence of ECU license agreements for agricultural equipment.

Finally, opponents challenge proponents' proposition that making copies of computer programs on ECUs is an essential step in the utilization of the computer program in conjunction with a machine.[1539] In opponents' view, proponents cannot demonstrate that diagnosis, repair and modification activities will be limited merely to adding new features and capabilities to the software in the manner contemplated by *Krause*.[1540] Similarly, they challenge the notion that the proposed copying will fit within the archival purposes exception of section 117(a)(2).[1541]

[1532] *See, e.g.*, Auto Alliance Class 21 Opp'n at 9-10; John Deere Class 21 Opp'n at 9; GM Class 21 Opp'n at 17-18.

[1533] John Deere Class 21 Opp'n at 9.

[1534] *See, e.g.*, Auto Alliance Class 21 Opp'n at 6-7; GM Class 21 Opp'n at 9-14; Global Automakers Class 21 Opp'n at 5-6.

[1535] *See, e.g.*, Auto Alliance Class 21 Opp'n at 6-7; GM Class 21 Opp'n at 9-14; Global Automakers Class 21 Opp'n at 5-6; John Deere Class 21 Opp'n at 5-6.

[1536] GM Class 21 Opp'n at 11-12 (citing *Krause*, 402 F.3d at 124; *Vernor*, 621 F.3d at 1110-11; 2010 Recommendation at 126).

[1537] *Id.* (citing EFF Class 21 Supp. at 13-14).

[1538] Tr. at 276:18-24 (May 19, 2015) (Lightsey, GM) ("I think it would be very difficult, if not impossible, to have license agreements covering the myriad of ECU's that are contained in the vehicle.").

[1539] GM Class 21 Opp'n at 12-13 (citing 17 U.S.C. § 117(a)(1)).

[1540] *Id.* at 13.

[1541] *Id.* at 13-14 (citing 17 U.S.C. § 117(a)(2)).

b. Asserted Adverse Effects

Opponents dispute that TPMs have a substantial adverse impact on the ability of vehicle owners to engage in lawful diagnosis, repair or modification of their vehicles.[1542] They assert that there is no need to circumvent as vehicle owners have alternative options that permit diagnosis and repair of their vehicles.[1543] While opponents do not focus on the modification element of the exemption, GM maintains that proponents have not demonstrated that a significant number of individuals are interested in accessing the software controlling a vehicle's ECUs for the purposes of modification.[1544]

To support their position, opponents reference a nationwide MOU entered into in January 2014 by major organizations representing automobile manufacturers, after market providers and auto repair services, including opponents Auto Alliance and Global Automakers.[1545] Opponents note that the MOU includes a "Right to Repair" commitment requiring the signing manufacturers and aftermarket service providers to make all diagnostic repair tools available to vehicle owners and independent repair facilities for all vehicles for model years 2002 forward.[1546] The Right to Repair commitment also includes requirements relating to tool standardization for vehicles starting with 2018 model year vehicles.[1547] Opponents maintain that, with few exceptions,[1548] this commitment guarantees independent vehicle repair facilities, and

[1542] *See, e.g.*, Auto Alliance Class 21 Opp'n at 11-16; GM Class 21 Opp'n at 18-20; John Deere Class 21 Opp'n at 10-12.

[1543] *See, e.g., id.*

[1544] GM Class 21 Opp'n at 19.

[1545] Auto Alliance Class 21 Opp'n at 12-16, App. A (MOU).

[1546] *Id.* at 13, App. A (MOU & R2R Agreement) (Section 2(a) of the R2R Agreement states, "for Model Year 2002 motor vehicles and thereafter, a manufacturer of motor vehicles sold in United States shall make available for purchase by owners of motor vehicles manufactured by such manufacturer and by independent repair facilities the same diagnostic and repair information, including repair technical updates, that such manufacturer makes available to its dealers through the manufacturer's internet-based diagnostic and repair information system or other electronically accessible manufacturer's repair information system. All content in any such manufacturer's repair information system shall be made available to owners and to independent repair facilities in the same form and manner and to the same extent as is made available to dealers utilizing such diagnostic and repair information system. Each manufacturer shall provide access to such manufacturer's diagnostic and repair information system for purchase by owners and independent repair facilities on a daily, monthly and yearly subscription basis and upon fair and reasonable terms.").

[1547] *Id.* at 13; *see id.* at App. A (R2R Agreement) (providing that "[c]ommencing in Model Year 2018, except as provided in subsection (2)(e), manufacturers of motor vehicles sold in the United States shall provide access to their onboard diagnostic and repair information system . . . using an off-the-shelf personal computer" and a non-proprietary vehicle interface).

[1548] *See, e.g., id.* at 14-16 (conceding instances in which owners of older vehicles, such as a 1987 Cadillac, would not be covered by the MOU, and an instance in which Subaru refused to provide an independent repair shop with the computer program for a low tire pressure sensor).

individual vehicle owners who wish to patronize such facilities, access to the information necessary to engage in the desired diagnostic and repair activities.[1549]

c. Argument Under Statutory Factors

With respect to section 1201(a)(1)'s statutory factors, opponents assert that the first factor, concerning the availability for use of copyrighted works, is not substantially impacted by the current prohibition on circumvention.[1550] They assert that granting the proposed exemption would not substantially advance the availability for use of the copyrighted works because numerous alternatives to circumvention exist for the proposed activities.[1551]

Opponents devote little time to the second factor, but generally maintain that the proposed exemption is wholly unrelated to the availability for use of works for nonprofit archival, preservation, and educational purposes.[1552] Similarly, with respect to the third factor, opponents assert that the proposed exemption would not impact criticism, comment, news reporting, teaching, scholarship or research.[1553]

Regarding the fourth statutory factor, opponents maintain that the effect of the exemption on the market for or value of copyrighted works would generally be negative,[1554] asserting that the exemption would erode public confidence in the safety and security of vehicles.[1555] GM in particular suggests that the exemption would create public concern about U.S. efficacy in regulating vehicles, and uncertainty as to whether a subsequent purchaser could trust a vehicle's ECU system since it may have been modified by a prior owner.[1556] As a result, according to opponents, granting the exemption could lead to a diminishment in the value of the vehicles and their associated software.

Opponents also raise specific concerns regarding entertainment and telematics system ECUs. GM notes that "[v]ehicle entertainment systems can include non-software copyrighted content, such as videogames, music and movies, as well as other digital content."[1557] In the case of telematics, opponents note that GM's OnStar and other telematics systems typically require an ongoing subscription.[1558] Auto Alliance explains

[1549] *See, e.g.*, *id.* at 13-16; GM Class 21 Opp'n at 19-20.

[1550] GM Class 21 Opp'n at 21; John Deere Class 21 Opp'n at 11-12.

[1551] GM Class 21 Opp'n at 21; John Deere Class 21 Opp'n at 10-12.

[1552] GM Class 21 Opp'n at 13, 21-22; John Deere Class 21 Opp'n at 12-13.

[1553] GM Class 21 Opp'n at 22; John Deere Class 21 Opp'n at 13.

[1554] GM Class 21 Opp'n at 22-23; John Deere Class 21 Opp'n at 13.

[1555] GM Class 21 Opp'n at 23; John Deere Class 21 Opp'n at 13.

[1556] GM Class 21 Opp'n at 23.

[1557] GM Class 21 Post-Hearing Resp. at 1.

[1558] *See, e.g.*, Tr. at 279:06-17 (May 19, 2015) (Charlesworth, USCO; Lightsey, GM).

that "removing the prohibition on circumvention of access controls on vehicle software could enable unauthorized access to [such] value added services without any payment, or could allow [unauthorized] access to premium content."[1559]

Opponents rest much of their argument against the exemption on the fifth statutory factor, which permits consideration of "such other factors as the Librarian considers appropriate."[1560] They assert that the proposed exemption would negatively impact vehicle safety, energy policy (including fuel efficiency), the environment (including air pollution and the emission of greenhouse gas pollutants), personal security (including cybersecurity), and consumer reliance on the integrity of vehicle design and operation.[1561] Additionally, through a letter offered at the hearing by Auto Alliance, the National Network to End Domestic Violence expressed its concern that the proposed exemptions would make it easier for violent partners and predators to monitor, stalk, and harm victims through access to what is now protected internal automobile systems and technology.[1562] Opponents also argue that both state and federal regulatory regimes are designed to prevent many of the activities that would fall within the exemption. In particular, they point out that commercial providers are prohibited from knowingly modifying vehicles to take them out of compliance with emissions and safety standards.[1563]

Opponents acknowledge that it is difficult to quantify the potential negative impacts on the existing regulatory regime.[1564] They also recognize that not all of the activities allowed under the exemption would necessarily have deleterious effects on compliance with regulatory standards.[1565] They assert, however, that negative impacts would appear to be an inescapable consequence of allowing unrestricted modification of vehicle ECUs.[1566] Additionally, they suggest that if the Librarian were to create an exemption to allow circumvention of what are now legally protected TPMs, the public

[1559] Auto Alliance Class 21 Post-Hearing Resp. at 1.

[1560] 17 U.S.C. § 1201(a)(1)(C)(v); *see also, e.g.*, GM Class 21 Opp'n at 23-24; Global Automakers Class 21 Opp'n at 6-8; John Deere Class 21 Opp'n at 14-15; Auto Alliance Class 21 Opp'n at 16-21.

[1561] *See, e.g.*, GM Class 21 Opp'n at 23-24; Global Automakers Class 21 Opp'n at 6-8; John Deere Class 21 Opp'n at 14-15; Auto Alliance Class 21 Opp'n at 16-21; Tr. at 27:15-28:20 (May 19, 2015) (Lightsey, GM).

[1562] Letter from Cindy Southworth, Exec. Vice President and Founder of the Safety Net Tech. Project at Nat'l Network to End Domestic Violence to Jacqueline C. Charlesworth, Gen. Counsel and Assoc. Register of Copyrights, USCO, at 1 (May 18, 2015).

[1563] Auto Alliance Class 21 Opp'n at 16-17 (citing 42 U.S.C. § 7522(a)(3) (knowingly removing or rendering inoperative after delivery to the purchaser "any device or element of design" installed in or on a motor vehicle in compliance with emissions standards regulations is prohibited); 49 U.S.C. § 30122(b) (providing that "motor vehicle repair business[es] [as well as dealers] may not knowingly make inoperative any part of a device or element of design installed on or in a motor vehicle or motor vehicle equipment in compliance with an applicable motor vehicle safety standard")).

[1564] *See, e.g., id.*

[1565] *See, e.g., id.* at 18-19.

[1566] *See, e.g., id.* at 19.

will perceive the exemption as a government endorsement of unrestricted modification of vehicles, notwithstanding any other laws or regulations that might prohibit those activities.[1567] Opponents also suggest that the proposed exemption could raise product liability issues because the exemption would make it difficult to determine whether modifications to ECUs were contributing factors in accidents.[1568] In addition, opponents urge that "software manipulation in a vehicle is typically undetectable by most consumers" and that a downstream purchaser of a used automobile would not know whether any software modifications had been made.[1569]

Finally, opponents recognize that the non-copyright factors that they identify have not played a significant role in the Register's consideration of proposed exemptions in prior rulemakings.[1570] But, they urge that the instant exemption is different because of its potential to impact the highly regulated automotive sector directly.[1571]

3. Discussion

a. Noninfringing Uses

The Register concludes that the overall record supports proponents' claim that reproducing and altering the computer programs on ECUs for purposes of facilitating diagnosis, repair and modification of vehicles may constitute a noninfringing activity as a matter of fair use and/or under the exception set forth in section 117.

i. Fair Use

Regarding the first factor of fair use, the record establishes that the purpose and character of the proposed uses tend to support a finding of fair use because at least some of the proposed uses of ECU computer programs are likely to be transformative. These uses include copying the work to create new applications and/or tools that can interoperate with ECU software and facilitate functionalities such as diagnosis, modification and repair.[1572] Such uses may also extend to modification of ECU computer programs to "interoperate" with different auto parts.[1573]

While it is often a negative factor in the fair use analysis, a finding of fair use is not necessarily precluded when the new use coincides generally with the original use of a work. In the course of recommending an exemption for the "jailbreaking" of

---

[1567] *See, e.g., id.* at 17.

[1568] *Id.* at 20.

[1569] GM Class 21 Post-Hearing Resp. at 2; *see also* GM Class 21 Opp'n at 6-7.

[1570] Auto Alliance Class 21 Opp'n at 16, 20-21.

[1571] *Id.*

[1572] *See, e.g.*, EFF Class 21 Supp. at 8.

[1573] *Cf.* 2010 Recommendation at 93-94 (noting that uses that enable interoperability are favored under the first factor).

smartphones, for example, the Register previously concluded that the first factor may favor fair use where "the purpose and character of the use is noncommercial and personal" and facilitates the intended use of smartphones by their owners.[1574] Here, similarly, the proposed uses for diagnosis and repair would presumably enhance the intended use of ECU computer programs.

At the same time, the record supports distinguishing ECUs that are chiefly designed to operate vehicle entertainment and telematics systems. Access controls on entertainment system ECUs not only preserve the integrity of the ECU itself, but also protect the content that is played through the entertainment system. Telematics systems, too, rely on TPMs to protect proprietary offerings. Opponents' concerns of unauthorized access to the content made available through such systems were not effectively rebutted by proponents. The record is sparse concerning noninfringing uses that would be facilitated by allowing circumvention of the TPMs protecting these systems.[1575] The focus of proponents' request was instead on ECUs used to control vehicle functions like ignition, gear shifting, and engine power.[1576] Thus, the Register finds that, on the current record, the first factor is generally favorable to proponents, except with respect to ECU computer programs that are primarily designed to support vehicle entertainment and telematics systems.

Concerning the second factor, the nature of the work, opponents generally recognize the Register's established position that computer programs such as those contained in ECUs are essentially functional works used to operate a device.[1577] Although opponents urge the Register to treat vehicle software differently, the Register is unable to discern a meaningful difference between computer programs used to operate a vehicle and those used to operate a phone.[1578] Vehicle software is at least as functional as a phone's operating system, in that it is used to support operational and mechanical processes. Contrary to opponents' view, vehicle software is not especially "expressive;" it is not meant to be consumed as a creative work. The Register therefore concludes that the second fair use factor favors a finding of fair use.

In addressing the third factor, which considers the amount of the work used, proponents concede that in most cases the proposed uses would involve reproduction of copyrighted computer programs in their entirety, and there is nothing in the record to

[1574] 2012 Recommendation at 74.

[1575] In response to post-hearing questions, EFF states that "[i]t is important that the vehicle software of telemetry and entertainment systems be accessible under the proposed exemption." EFF Class 21 Post-Hearing Resp. at 1. But EFF fails to offer specific noninfringing uses that would be facilitated by extending the exemption.

[1576] *See, e.g.*, EFF Class 21 Supp. at 2.

[1577] *See, e.g.*, Auto Alliance Class 21 Opp'n at 8 (citing 2012 Recommendation at 73); John Deere Class 21 Opp'n at 7-8.

[1578] *See* 2012 Recommendation at 73.

suggest otherwise.[1579] As EFF observes, however, courts have been willing to permit extensive copying of the original work where it is necessary to accomplish a transformative purpose.[1580] Thus, while the third factor arguably disfavors a fair use finding, the weight to be given to it under the circumstances is slight.

Factor four, regarding the effect on the market for or value of the copyrighted work, is concerned with market substitution and includes evaluating "not only the extent of market harm caused by the particular actions of the [user], but also whether unrestricted and widespread conduct of the sort engaged in by the [proponent of fair use] . . . would result in a substantially adverse impact on the potential market."[1581] Proponents persuasively establish that computer programs on the majority of ECUs are only meaningful in connection with the vehicle, that the copies are generally sold only with the vehicle, and that the consumer pays for those copies when purchasing the vehicle. Indeed, some of the opponents themselves recognize that "there is no separate market for the computer programs and other works at issue here aside from the vehicle in which they are embedded."[1582] Proponents have thus established that there is not a significant independent market for ECU computer programs that can be harmed.[1583]

Opponents, however, point to the potential negative impact on the public's trust in the safety and security of vehicles in which the computer programs exist,[1584] and John Deere goes on to assert a consequential depressive effect on the secondary market for automobiles.[1585] But the Register finds opponents' concerns regarding reputational harms due to modification and repair activities to be unsupported and speculative. Vehicle owners have long repaired and modified their automobiles and farm equipment—adjusting brakes and enhancing suspensions, for example—including before the advent of computerized vehicle systems. It is thus not readily apparent these activities would cause unusual or undue harm. Moreover, opponents fail to identify actual instances in which repairs or modifications involving ECU software have affected resale values. Nor do opponents explain how modified ECU computer programs in existing vehicles would adversely impact the market for ECU computer programs in new vehicles offered by a manufacturer. In sum, at least on the record in this proceeding, opponents have failed to establish market harm.

[1579] *See, e.g.*, IPTC USC Class 21 Supp. at 12; EFF Class 21 Supp. at 10.

[1580] EFF Class 21 Supp. at 10; *see also HathiTrust*, 755 F.3d at 98 ("For some purposes, it may be necessary to copy the entire copyrighted work, in which case Factor Three does not weigh against a finding of fair use."); *Kelly v. Arriba Soft Corp.*, 336 F.3d 811, 820-21 (9th Cir. 2003) (holding that the third fair use factor did not weigh against copier when entire-work copying was reasonably necessary).

[1581] *Campbell*, 510 U.S. at 590 (internal quotations omitted).

[1582] IPTC USC Class 21 Reply at 10 (citing Auto Alliance Class 21 Supp. at 9).

[1583] EFF Class 21 Supp. at 11.

[1584] GM Class 21 Opp'n at 23; John Deere Class 21 Opp'n at 13.

[1585] *See, e.g.*, John Deere Class 21 Opp'n at 13; GM Class 21 Opp'n at 17-18.

On balance, the fair use analysis suggests that—with the exception of computer programs on ECUs that are primarily designed to operate vehicle entertainment and telematics systems—many of the proposed uses of ECU computer programs to facilitate diagnosis, repair and modification of vehicles, including agricultural machinery, are likely noninfringing under section 107.

ii. Section 117

Class 21 proponents argue that making copies and adaptations of vehicle computer programs is an essential step in the process of diagnosis, repair and modification and qualifies as a noninfringing use under section 117.[1586] Section 117 requires consideration of two questions in this context: whether a vehicle owner is also an owner of an embedded ECU computer program, and whether creating a new copy or adaptation of that program is an "essential step" in the utilization of the program with the vehicle.

In past rulemaking proceedings, the Register has reviewed case law governing the determination of ownership of a copy of a computer program for purposes of section 117 when formal title is lacking and/or a license or agreement imposes restrictions on the use of the computer program, and has concluded that the application of the law may be unclear in some contexts.[1587] The Register has observed that while *Vernor v. Autodesk, Inc.*[1588] and *Krause v. Titleserv, Inc.*[1589] may provide "useful guideposts," they are "controlling precedent in only two circuits and are inconsistent in their approach."[1590]

In *Krause*, the Second Circuit held that formal title was not necessary to demonstrate ownership under section 117 and that courts should look to a range of factors to determine whether a party "exercises sufficient incidents of ownership over a copy of the program to be sensibly considered the owner of the copy."[1591] These factors include: (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.[1592] By

[1586] *See, e.g.*, EFF Class 21 Supp. at 13.

[1587] *See* 2010 Recommendation at 90, 129 ("[T]he law relating to who is the owner of a copy of a computer program under [s]ection 117 is in flux."); 2012 Recommendation at 92 ("The Register concludes that the state of the law remains unclear.").

[1588] 621 F.3d 1102.

[1589] 402 F.3d 119.

[1590] 2012 Recommendation at 92.

[1591] *Krause*, 402 F.3d at 124.

[1592] *Id.*

contrast, in *Vernor*, the Ninth Circuit held that "a software user is a licensee rather than an owner of a copy where the copyright owner (1) specifies that the user is granted a license; (2) significantly restricts the user's ability to transfer the software; and (3) imposes notable use restrictions."[1593] These tests remain the two dominant approaches to the question of whether computer programs are owned or licensed by the user.

Under either test, the record here supports the conclusion that in many cases vehicle owners own the ECU computer programs. The record includes a few license agreements that address a narrow selection of ECUs designed for telematics or entertainment purposes. These types of systems control or contain copyrighted content, such as music or other creative works, beyond the computer programs that are the focus of the proposed exemption.[1594] Beyond these few license agreements—which, under relevant case law, are not definitive—opponents offered little evidence to support the notion that copies of computer programs on vehicles are merely licensed to the vehicle owner.[1595] Opponents point to no significant explicit restrictions on owners' use or resale of ECU computer programs.[1596] Thus, based on the record, at least some vehicle owners would seem to qualify as "owners" of ECU software, at least with respect to computer programs that that are not chiefly designed to operate vehicle entertainment or telematics systems.

The record further establishes that reproduction and alteration of ECU computer programs are very often an "essential step" in the process of vehicle diagnosis, repair and modification.[1597] In order to understand the functioning of a computer program, one must often make a copy to use in conjunction with a "machine" such as a diagnostic tool or general-purpose computer, on which the programs will be analyzed. The proposed uses also appear consistent with one of the purposes of section 117 as reflected in the Final Report of the National Commission on New Technological Uses of Copyrighted Works ("CONTU")—namely, "the right to add features to the program that were not present at the time of rightful acquisition."[1598] This purpose is echoed in *Krause*, which held that section 117 encompasses not only modifications to computer programs that are

[1593] *Vernor*, 621 F.3d at 1111.

[1594] *See, e.g.*, EFF Class 21 Supp. at 13-14; Tr. at 277:13-23 (May 19, 2015) (Walsh, EFF).

[1595] Tr. at 183:02-12 (May 19, 2015) (Walsh, EFF).

[1596] *See, e.g.*, EFF Class 21 Reply at 9-10 ("The purchaser may dispose of the vehicle along with the ECUs inside whenever the purchaser wishes. Vehicle manufacturers generally do not retain the right to repossess vehicle ECUs from their purchasers. Aside from a small number of narrow end user license agreements pertaining to media and telematics systems, there is no evidence in the record that manufacturers restrict the vehicle owner's ability to transfer the firmware or impose notable restrictions upon the user of the firmware.").

[1597] *See, e.g.*, EFF Class 21 Supp. at 15; EFF Class 21 Reply at 10; IPTC USC Class 21 Reply at 7.

[1598] CONTU, FINAL REPORT OF THE NATIONAL COMMISSION ON NEW TECHNOLOGICAL USES OF COPYRIGHTED WORKS at 13 (1978).

"strictly necessary to keep the programs functioning," but also those that are "designed to improve their functionality."[1599]

Additionally, proponents have established that the creation of backup copies of ECU computer programs to protect against destruction or damage may well be covered by the provision allowing the creation of copies for archival purposes.[1600] Based on the record submitted, it is therefore likely that many of the proposed uses of ECU software qualify as protected uses under section 117.

b. Adverse Effects

Both proponents and opponents agree that a significant number of vehicle manufacturers employ TPMs to control access to ECU computer programs. Proponents present a compelling case to establish that in many instances, these TPMs have a substantial adverse impact on the ability of vehicle owners to engage in diagnosis, repair or modification of their vehicles.[1601] Although some repair and diagnostic activities can be conducted through the use of manufacturer-licensed tools or services, proponents provide evidence demonstrating that those alternatives may be less accessible and/or substantially more costly. In the case of farm equipment in particular, proponent iFixit submitted evidence that the current prohibition sometimes requires farmers to wait a significant period of time for repairs by an authorized technician, impeding their productivity. Moreover, the record shows that manufacturer-licensed tools and services may not facilitate all modifications of vehicles; for example, the record indicates that manufacturer-licensed tools will only allow modifications within manufacturer-defined calibrations, and may not allow for certain modifications such as changes to the axle bearing.[1602] Additionally, the record indicates that manufacturer-licensed tools may not identify the underlying cause of a needed repair, such as in the example of the faulty communications system in the power window unit.[1603] Opponents focus much of their commentary on illicit modifications, such as disabling of emissions controls. While as discussed at some length below, this is certainly a concern, it must be remembered that many modifications of vehicles—not to mention diagnostic tests and repairs—are perfectly lawful.

[1599] *Krause*, 402 F.3d at 126.

[1600] *See, e.g.*, EFF Class 21 Reply at 11-12.

[1601] EFF Class 21 Supp. at 17 (citing Jonathan Welsh, *Is the Dealer Better Than an Independent Mechanic?*, WALL ST. J. (May 17, 2010), http://blogs.wsj.com/drivers-seat/2010/05/17/is-the-dealer-better-than-an-independent-mechanic (discussing study showing that consumers can save an average of about $300 a year, or 25% of their maintenance and repair bills, by going to an independent repair shop) and *Where to Repair? Dealer or Independent*, CAR TALK, http://www.cartalk.com/content/where-repair-dealer-or-independent (last visited Oct. 7, 2015) (finding that dealers charged 15% more than independent repair shops for the same repairs)).

[1602] Tr. at 218:02-13 (May 19, 2015) (Damle, USCO; Douglas, Auto Alliance).

[1603] *Id.* at 222:09-20 (Smith, Open Garages).

Opponents suggest that any adverse effects stemming from the prohibition on circumvention are mitigated by the nationwide MOU that is intended to facilitate access to authorized tools and information needed to engage in diagnostic and repair activities.[1604] While it is an encouraging development, the record nonetheless suggests that the MOU cannot fully address the cited adverse impacts.[1605] Among other things, proponents convincingly explain that the MOU does not apply to a significant portion of the vehicles that would be covered by the proposed exemption, including pre-2002 models and mechanized agricultural vehicles.[1606]

In light of this record, the Register concludes that TPMs protecting computer programs on ECUs have a substantial adverse impact on the ability of vehicle owners to engage in lawful diagnosis, repair and modification of their vehicles.

c. Statutory Factors

The Register finds that the first factor, concerning the availability for use of copyrighted works,[1607] is neutral. While proponents assert that allowing circumvention will allow greater "use" of the works to which the TPMs at issue apply, this logic is circular in that the same could presumably be said of any work sought to be accessed for a particular use. The more salient consideration is whether the exemption will lead to greater availability of copyrighted works in the marketplace. Here, the record indicates that the use of ECU software is tied to vehicle ownership; there is no evidence that the purchase of vehicles would be impacted by the exemption. Moreover, as opponents observe, the works in question are already available for use because drivers rely upon them to operate their vehicles.[1608]

Turning to the second factor, the availability for use of works for nonprofit archival, preservation, and educational purposes,[1609] the Register finds that this factor likewise is not especially relevant to this exemption. Although proponents state that users will make personal backup copies in the course of engaging in diagnosis, repair or modification,[1610] it is not apparent that this is the sort of "archival" use that the factor is aimed at protecting. Rather, as used in the context of section 1201(a)(1), the term "archival," which is modified by "nonprofit" and appears in conjunction with

---

[1604] *See, e.g.*, Auto Alliance Opp'n at 12-15, Exhibit A (MOU and Right to Repair Agreement), Exhibit B (Dorgan Letter); GM Class 21 Opp'n at 19 (referring to MOU); Tr. at 213:21-214:09, 215:03-216:20 (May 19, 2015) (Damle, USCO; Douglas, Auto Alliance) (discussing MOU, Right to Repair Agreement, Dorgan Letter, California Air Resources Board and Environmental Protection Agency regulations).

[1605] *See, e.g.*, EFF Class 21 Reply at 17-18.

[1606] *See, e.g., id.*; IPTC USC Class 21 Reply at 12; Tr. at 228:25-229:01 (May 19, 2015) (Lightsey, GM).

[1607] 17 U.S.C. § 1201(a)(1)(C)(i).

[1608] Tr. at 213:18-214:14 (May 19, 2015) (Douglas, Auto Alliance).

[1609] 17 U.S.C. § 1201(a)(1)(C)(ii).

[1610] *See, e.g.*, EFF Class 21 Reply at 11-12.

"preservation[] and educational purposes," is better understood as referring to library-type "archives" akin to those covered in section 108.[1611]

With respect to the third factor, proponents have established that the exemption may to some degree enhance criticism, comment, news reporting, teaching, scholarship and research. Specifically, they convincingly explain that granting the exemption will enable efforts to educate the public about vehicle software systems and related matters, as in the case of the *Car Hacker's Handbook*.[1612] Thus, this factor weighs somewhat in favor of the exemption.

Regarding the fourth statutory factor—the impact of the proposed exemption on the market for or value of copyrighted works[1613]—the record is somewhat mixed. As noted above, proponents persuasively established that the market for vehicle computer programs does not exist apart from the market for the vehicles themselves; there was no evidence presented to demonstrate that circumvention would undermine the market for vehicles. Moreover, based on the record, opponents' claims of negative impacts on the public's trust in the safety and security of vehicles appear to be wholly speculative.[1614] At the same time, for the reasons set forth in the fair use analysis above, the record does support distinguishing ECU computer programs that control entertainment and telematics systems from those that control other operations in the vehicle; there is some evidence to suggest that circumvention of access controls on entertainment and telematics ECUs could result in a diminution in the value of copyrighted works if those systems could no longer reliably protect the content made available through them.[1615] In sum, the Register concludes that this statutory factor favors the proponents except perhaps with respect to computer programs on ECUs that are chiefly designed to operate telematics or entertainment systems.

Finally, the statute also permits the Librarian to consider "such other factors" as may be appropriate.[1616] As opponents note, the proposed exemption raises potentially serious policy concerns. The list of issues includes vehicle safety, energy policy (including fuel efficiency), the environment (including air pollution and emission of greenhouse gas pollutants), personal security (including cybersecurity), and consumer reliance on the integrity of vehicle design and operation.[1617] An additional concern

---

[1611] 17 U.S.C. § 1201(a)(1)(C)(ii); *see also id.* § 108.

[1612] EFF Class 21 Supp. at 23.

[1613] 17 U.S.C. § 1201(a)(1)(C)(iv).

[1614] John Deere Class 21 Opp'n at 9; GM Class 21 Opp'n at 17-18.

[1615] *See, e.g.*, Tr. at 268:12-271:16 (May 19, 2015) (Charlesworth, USCO; Walsh, EFF; Ruwe, USCO; Damle, USCO; Nabel, IPTC USC; Weins, iFixit; Metalitz, Auto Alliance).

[1616] 17 U.S.C. § 1201(a)(1)(C)(v).

[1617] *See, e.g.*, GM Class 21 Opp'n at 23-24; Global Automakers Class 21 Opp'n at 6-8; John Deere Class 21 Opp'n at 14-24; Auto Alliance Class 21 Opp'n at 16-21; Tr. at 27:15-28:20 (May 19, 2015) (Lightsey, GM); *see also* Tr. at 18:12-20 (May 19, 2015) (Miller) (describing his research on methods hackers can use to remotely control vehicles via the internet).

subject to debate in the record was whether purchasers of used vehicles would be able to identify and assess modifications to vehicle software made by a previous owner.[1618]

As opponents note, these sorts of safety and environmental concerns have not played a significant role in the Register's consideration of proposed exemptions in prior rulemakings.[1619] And proponents also point out with some force that such issues are relatively remote from the copyright interests that are at the heart of section 1201—namely, the ability to protect, disseminate and enjoy creative works in the digital age.[1620] At the same time, opponents correctly note that prior exemptions did not have the potential for the same type of direct impact on such a highly regulated sector as the automotive industry.[1621] Opponents emphasize that auto manufacturers are obligated to comply with a host of federal and state safety and environmental mandates, and that the use of TPMs has played a role in effectuating compliance.[1622]

In view of the significant public policy issues falling within the expertise and authority of other government agencies, and the concerns expressed by various commenting parties, the Copyright Office took steps to advise the Department of Transportation ("DOT") and the Environmental Protection Agency ("EPA") of the pending rulemaking.[1623] DOT and EPA submitted letters to the Office commenting on the proposed exemption, which are included in the record of this proceeding.[1624] And, although the Office had not specifically notified it of the pending proceeding, the

---

[1618] *Compare* EFF Class 21 Post-Hearing Resp. at 2-4 (proposing that manufacturers publish "checksums" for original ECU software to allow repair shops to confirm that no changes were made), *with* Auto Alliance Class 21 Post-Hearing Resp. at 1-2 (arguing that publishing checksums for every ECU software version would be a "massive undertaking" and would be "for naught" because a "moderately sophisticated hacker could determine the correct checksum and then simply hardcode the ECU to report that checksum value").

[1619] *See, e.g.*, Auto Alliance Class 21 Opp'n at 16, 20-21.

[1620] *See, e.g.*, IPTC USC Class 21 Reply at 14.

[1621] *See, e.g.*, Auto Alliance Class 21 Opp'n at 16.

[1622] *See, e.g., id.*

[1623] Letter from Jacqueline C. Charlesworth, Gen. Counsel and Assoc. Register of Copyrights, USCO to Kathryn B. Thomson, Gen. Counsel, DOT, and Stephen P. Wood, Acting Chief Counsel, Nat'l Highway Traffic Safety Admin. (May 12, 2015); Letter from Jacqueline C. Charlesworth, Gen. Counsel and Assoc. Register of Copyrights, USCO, to Avi S. Garbow, Gen. Counsel, EPA (May 12, 2015).

[1624] Letter from Geoff Cooper, Assistant Gen. Counsel, EPA, to Jacqueline C. Charlesworth, Gen. Counsel and Assoc. Register of Copyrights, USCO (July 17, 2015) ("EPA Letter"); Letter from Kathryn B. Thomson, Gen. Counsel, DOT, to Jacqueline C. Charlesworth, Gen. Counsel and Assoc. Register of Copyrights, USCO (September 9, 2015) ("DOT Letter"). The letters to and from the agencies are available at http://copyright.gov/1201/2015/USCO-letters. Consideration of these agency responses is appropriate because the matter of other agencies' potential concerns with respect to this exemption was raised by commenting parties and has been part of the record since the filing of opposition comments on March 27, 2015. *See, e.g.*, John Deere Class 21 Opp'n at 20-23. These concerns were also raised at the public hearings. Tr. at 56:05-57:16 (May 19, 2015) (Charlesworth, USCO; Lightsey, GM). Proponents thus had the opportunity to address these concerns both in their reply comments and at the public hearings, and the record reflects significant public input on these issues in this class.

California Air Resources Board ("California ARB") submitted a letter as well.[1625] As explained below, DOT, EPA, and California ARB all expressed significant reservations about the proposed exemption. NTIA, however, fully supported adoption of the proposed exemption.[1626]

In its letter, DOT noted that permitting individuals to modify vehicle software could create safety and cybersecurity risks, which would be contrary to the purposes of the National Traffic and Motor Vehicle Safety Act ("NTMVSA").[1627] DOT further observed that vehicle modifications could create significant safety risks not only to the operators of modified vehicles, but also to occupants of other cars, as well as to pedestrians and cyclists.[1628] DOT noted that the NTMVSA contains prohibitions against certain types of tampering, namely with vehicle components that are regulated by the Federal Motor Vehicle Safety Standards ("FMVSS").[1629] At the same time, DOT explained that many safety-critical functions may not be directly regulated by FMVSS and that tampering with computer programs that control those unregulated functions would not violate the NTMVSA.[1630] Finally, DOT noted that the NTMVSA prohibitions apply narrowly to motor vehicle manufacturers, distributors, dealers and repair businesses, but not to other persons.[1631]

EPA's submission urged the Register to decline to recommend the proposed exemption, expressing concern that granting the exemption "would enable actions that could slow or reverse gains under the Clean Air Act."[1632] EPA explained that the Clean Air Act ("CAA") and its implementing regulations "are responsible for a significant reduction in harmful emissions from motor vehicles," and that "[c]omputer programs installed on motor vehicles, controlling engine operations and minimizing emissions under a variety of conditions, have been critical to achieving the reduction."[1633] It observed that its own enforcement activities indicate that "the majority of modifications to engine software are being performed to increase power and/or boost fuel economy."[1634] According to EPA, "[t]hese kinds of modifications will often increase emissions from a vehicle engine, which would violate section 203(a) of the CAA, commonly known as the 'tampering prohibition.'"[1635] In addition, EPA expressed concern that the exemptions

[1625] Letter from Alberto Ayala, Deputy Exec. Officer, California ARB, to Jacqueline C. Charlesworth, Gen. Counsel and Assoc. Register of Copyrights, USCO (July 21, 2015) ("California ARB Letter").

[1626] 17 U.S.C. § 1201(a)(1)(C).

[1627] DOT Letter at 2.

[1628] *Id.*

[1629] *Id.*

[1630] *Id.*

[1631] *Id.*

[1632] EPA Letter at 1-2.

[1633] *Id.* at 2.

[1634] *Id.*

[1635] *Id.*

would "hinder its ability to enforce the tampering prohibition."[1636] EPA explained that the agency "has taken enforcement action against third-party vendors who sell or install equipment that can 'bypass, defeat, or render inoperative' software designed to enable vehicles to comply with CAA regulations."[1637] EPA thus concluded that it "can curb this practice more effectively if circumventing TPMs remains prohibited under the DMCA."[1638]

California ARB echoed several of the same concerns with the Class 21 exemption.[1639] It indicated that in its estimation, the proposed exemption would not further the goal of improving fuel efficiency or vehicle performance, but would instead negatively impact emissions.[1640] It added that the proposed activity could undermine existing emissions control programs across the United States, as such programs will increasingly rely on TPMs.[1641] California ARB also expressed doubt as to whether an exemption is necessary for the proposed maintenance and repair activities.[1642]

Taking into account the issues raised by opponents, as well as the views of the agencies most closely associated with the regulation of motor vehicles, the Register is persuaded that on balance, the fifth statutory factor presents serious "other factors" that weigh against an exemption.

Accordingly, of the statutory factors set forth in section 1201(a)(1) that the Librarian and the Register are to consider, the Register finds that an analysis of the first four factors shows them to be neutral or to favor an exemption, while the final factor weighs against lifting the ban on circumvention.

4. NTIA Comments

NTIA, like the Register, concludes that "proponents have shown that the intended use of computer programs embedded in vehicles is likely to be noninfringing under fair use principles as well as Section 117" and that an exemption "would enable the longstanding practices that auto enthusiasts and mechanics engage in to modify their

---

[1636] *Id.* at 3.

[1637] *Id.*

[1638] *Id.* The Register further notes that to the extent EPA or another federal or state agency itself seeks to investigate—or appoint agents to investigate—alleged violations of the law, that agency should be able to rely on the permanent exception set forth in section 1201(e) for law enforcement activities, which allows "lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State." 17 U.S.C. § 1201(e).

[1639] *See generally* California ARB Letter.

[1640] *Id.* at 2-3.

[1641] *Id.* at 3-5.

[1642] *Id.* at 4.

vehicles to continue."[1643] At the same time, NTIA acknowledges that "some regulatory agencies" have "express[ed] concerns that modifications and repairs could cause vehicles to fall out of regulatory compliance with emission standards."[1644] NTIA also makes note of the potential safety and security issues highlighted by opponents, "including the ability to bypass the locks on video displays when the user is actively driving, illegal odometer tapping, the ability to bypass anti-theft systems, disabling the brakes, and falsifying speedometer readings."[1645]

Ultimately, however, NTIA concludes that the "non-copyright concerns" raised by opponents and other agencies are not a reason to deny the exemption.[1646] NTIA acknowledges that the fifth statutory factor in section 1201(a)(1)(C) broadly permits the Librarian to consider "such other factors as the Librarian considers appropriate."[1647] NTIA also acknowledges that non-copyright concerns have been relevant to proposed exemptions in past rulemakings, highlighting in particular the competition and telecommunications policies supporting past cellphone unlocking exemptions.[1648] Nevertheless, NTIA urges that the "deliberative process [in this rulemaking] should not deviate too far afield from copyright policy concerns."[1649]

Accordingly, while NTIA stresses that it is "sympathetic" to the safety and environmental concerns raised by opponents and other federal agencies, it expresses the "belie[f] that the appropriate regulatory authorities will continue to ensure compliance with federal and state laws that control safety features and emission."[1650] It also proposes "including a provision in the exemption explicitly stating that it does not preclude liability under other applicable laws."[1651]

While finding the safety and environmental concerns an insufficient basis to deny the exemption outright, NTIA acknowledges that the Register "may understandably be apprehensive about recommending exemptions that could inadvertently implicate [such] issues."[1652] NTIA thus recognizes that "[o]ne possible way forward may be to delay the date upon which such an exemption would become effective to allow the relevant

[1643] NTIA Letter at 54. Unlike the Register, NTIA does not separately analyze entertainment and telematics ECUs. *Id.* at 52-58. In addition, while NTIA's proposed regulatory language provides that circumvention will be permitted when conducted "at the request of the owner," it does not address whether such a provision is consistent with the anti-trafficking provisions set forth in section 1201(a)(2) and (b). *Id.* at 58.

[1644] *Id.* at 57.

[1645] *Id.*

[1646] *Id.* at 58.

[1647] *Id.* at 4 (citing 17 U.S.C. § 1201(a)(1)(C)(v)).

[1648] *Id.* at 3-4 & n.2.

[1649] *Id.* at 4.

[1650] *Id.* at 57.

[1651] *Id.* at 58.

[1652] *Id.* at 5.

stakeholders in other policy spheres to prepare for the exemption's effective date."[1653] While expressing doubt about whether "such a delay would be helpful," NTIA nonetheless notes this as a possible solution and, should it factor into the Register's recommendation, "urges the Copyright Office to keep any delay as short as practicable."[1654]

As discussed below, the Register agrees that an exemption should be granted, but that the serious safety and environmental concerns raised by other agencies must be accommodated by allowing a twelve-month period before it becomes effective.

5. Conclusion and Recommendation

Class 21 proponents have demonstrated that owners of personal automobiles, commercial motor vehicles, and agricultural machinery are adversely impacted in their ability to diagnose, repair and modify their vehicles as a result of TPMs that protect the copyrighted computer programs on the ECUs that control the functioning of the vehicles. They have also established that many of the uses in which the users seek to engage are likely to be noninfringing. Additionally, two of the five statutory factors tend to favor the proponents, two are neutral, and one weighs against the exemption. The Administration appears to have disparate views concerning the desirability of an exemption: while NTIA is in favor of an exemption, DOT and EPA (along with California ARB) have expressed serious reservations. Faced with a mixed record and sharply conflicting policy choices that are outside the purview of copyright, the Register recommends that an exemption be granted, but with careful limitations.

First, the recommended exemption excludes ECUs that are chiefly designed to operate entertainment and telematics systems. As explained above, proponents' request is largely focused on the computer programs on ECUs that control the vehicle's mechanical operation, not entertainment systems used to consume copyrighted content or telematics services that offer proprietary subscription services. There was insufficient evidence in the record to support a need for circumvention of the TPMs on these ECUs, especially when balanced against concerns about unauthorized access to the services and content they protect.

Second, the proposed exemption would allow circumvention not only by a vehicle owner, but also "on behalf of" the owner.[1655] While the Register is sympathetic to the practical issues that may arise if vehicle owners do not have the knowledge or ability to circumvent TPMs themselves, the phrase "on behalf of" may implicate the anti-trafficking provisions set forth in section 1201(a)(2) and (b).[1656] Section 1201(a)(1)

[1653] *Id.*

[1654] *Id.*

[1655] *See* EFF Vehicle Software Repair Pet. at 1; NPRM, 79 Fed. Reg. at 73,869.

[1656] 17 U.S.C. § 1201(a)(2), (b). The anti-trafficking rules set forth in section 1201(a)(2) and (b) generally prohibit the manufacture and provision of technologies, products or services—or "part[s] thereof"—that are "primarily" designed for purposes of circumvention. *Id.*

grants the Librarian of Congress the authority to adopt exemptions that apply to the prohibition on circumvention of technological measures that control access to copyrighted works, but does not grant authority to adopt exemptions that permit trafficking in circumvention tools or services.[1657] This limitation was expressly acknowledged by proponent EFF in connection with another class being considered in this proceeding; in its filing for Class 22, EFF correctly observed that "[t]o the extent that disclosure of information or release of circumvention tools constitute trafficking under other provisions of Section 1201, any exemption the Librarian grants cannot reach those activities."[1658]

A similar issue was present in the exemption for the unlocking of cellphones, which the Librarian granted in a manner consistent with section 1201(a)(1), expressly allowing only circumvention initiated by the owners of computer programs on the phones.[1659] In order to broaden the exemption to allow circumvention "by another person at the direction of the owner," Congress intervened, passing the Unlocking Consumer Choice and Wireless Competition Act ("Unlocking Act").[1660] The fact that Congress felt compelled to take this action in connection with unlocking indicates that Congress believed it was necessary to amend the law to permit circumvention "at the direction of" an owner. Significantly, the Unlocking Act applies only in the context of exemptions that permit unlocking of cellphones and other wireless devices,[1661] and proponents do not argue otherwise.

As noted, some consumers may find it challenging to circumvent TPMs protecting the computer programs that control the functioning of their vehicles themselves. Congress could find such concerns worthy of the same type of specific accommodation provided in the Unlocking Act. At present, however, neither section 1201 nor the Unlocking Act authorizes the Librarian of Congress to adopt exemptions that would allow circumvention to be performed by third parties on behalf of those who are actually entitled to an exemption. The Register therefore must decline to recommend that the exemption extend to circumvention "on behalf of" the vehicle owner.[1662]

[1657] Moreover, section 1201(a)(1)(E) expressly provides that determinations made in the triennial rulemaking proceeding may not "be used as a defense in any action to enforce any provision of this title other than [section 1201(a)(1)]." *Id.* § 1201(a)(1)(E); NOI, 79 Fed. Reg. at 55,688 n.2.

[1658] EFF Class 22 Supp. at 15 (citing 2010 Recommendation at 170-71).

[1659] 2012 Final Rule, 77 Fed. Reg. at 65,264-66. The 2010 cell phone unlocking exemption also had a similar limitation. *See* 2010 Final Rule, 75 Fed. Reg. at 43,830-32.

[1660] Unlocking Act, Pub. L. No. 113-144, § 2(c), 128 Stat. 1751, 1751-52 (2014).

[1661] S. REP. NO. 113-212, at 6-7 (2014).

[1662] As discussed above, the record indicates that it is likely that, under relevant precedent, the vehicle owner would also be considered the owner of at least the non-entertainment and non-telematics ECU software in the vehicle. Moreover, even if the vehicle owner is not the owner of the software, such a use by a vehicle owner is likely to be fair.

Third, the recommended exemption accounts for the serious policy concerns raised regarding potential safety and environmental impacts of an exemption. To be sure, as proponents urge, this rulemaking is principally focused on the copyright concerns implicated by any proposed exemption, and on that front, proponents have established the case for an exemption. At the same time, section 1201(a)(1) calls for consideration of "such other factors as the Librarian considers appropriate," and, while acknowledging NTIA's views, the Register believes it would be inappropriate simply to disregard other agencies' concerns regarding the possible negative impacts of the exemption on their respective regulatory and enforcement efforts.

Accordingly, the Register recommends two further refinements to the exemption to account for these legitimate safety and environmental concerns. The exemption should state explicitly that the diagnosis, repair or modification to be facilitated by the act of circumvention not violate any other law, including regulations promulgated by DOT or EPA. Thus, circumvention to achieve an illicit purpose—for example, to tamper with emissions controls in violation of applicable law—would not be permitted under the exemption.

The Register also recommends a delay of twelve months before the exemption goes into effect to allow other agencies with expertise in vehicle safety, environmental issues, and other relevant areas an opportunity to consider and react to the new rule. In keeping with the views of NTIA, the Register believes that a twelve-month delay is the shortest period that will reasonably permit other agencies to consider appropriate action.[1663]

Therefore, the Register recommends that the Librarian designate the following class:

> **Computer programs that are contained in and control the functioning of a motorized land vehicle such as a personal automobile, commercial motor vehicle or mechanized agricultural vehicle, except for computer programs primarily designed for the control of telematics or entertainment systems for such vehicle, when circumvention is a necessary step undertaken by the authorized owner of the vehicle to allow the diagnosis, repair or lawful modification of a**

[1663] The Register understands the Librarian to have the discretion necessary to phase in an exemption as required to address concerns in the record. Section 1201 allows the Librarian to deny exemptions outright, including based on the assessment of "such other factors as [he] considers appropriate" under the fifth statutory factor of section 1201(a)(1). *See* 17 U.S.C. § 1201(a)(1). Thus, the Librarian has the discretion to deny the proposed exemption at issue here, based on the substantial safety and environmental concerns presented in the record, with the understanding that it could be reconsidered in the next triennial proceeding. The Register, however, does not find outright denial to be necessary in this case. The Register understands the power to deny an exemption to carry with it the ability to designate a period of time before it becomes effective in lieu of denying the exemption entirely in order to address legitimate concerns in the record.

vehicle function; and where such circumvention does not constitute a violation of applicable law, including without limitation regulations promulgated by the Department of Transportation or the Environmental Protection Agency; and provided, however, that such circumvention is initiated no earlier than 12 months after the effective date of this regulation.

J. Proposed Classes To Permit Research of Software Flaws, Proposed Class 25: Software – Security Research; Proposed Class 22: Vehicle Software – Security and Safety Research; Proposed Class 27A: Medical Device Software – Security and Safety Research

1. Proposals

The Office received a number of petitions for proposed exemptions to permit circumvention of TPMs for the purposes of conducting good-faith testing for and the identification, disclosure and correction of malfunctions, security flaws, and vulnerabilities in computer programs.[1664] The Office uses the shorthand term "security research" to refer to these various activities. Although that term is sometimes used to refer narrowly to research into software flaws that render a system or device vulnerable to unauthorized access by third parties,[1665] the Office uses the term "security research" here in its broader sense also to include research into software flaws that cause a system or device to malfunction but do not necessarily involve such unauthorized access. The Office has grouped these security-related petitions into three proposed classes, as described below.

First, the Office received two submissions seeking an exemption to permit good-faith research into malfunctions, security flaws, or vulnerabilities in software installed on all types of systems and devices: one from Professor Matthew D. Green ("Green"),[1666] and the other from a group of academic security researchers comprising Professors Steven M. Bellovin, Matt Blaze, Edward W. Felten, J. Alex Halderman, and Nadia Heninger ("Bellovin et al.").[1667] The NPRM described the proposed class as follows:

[1664] The Register notes that throughout this Recommendation, the terms "firmware" and "software" are variously used, although both are "computer programs" within the meaning of the Copyright Act. *See* 17 U.S.C. § 101 (definition of "computer program").

[1665] *See, e.g.*, *Security and Privacy*, CARNEGIE MELLON UNIV., http://www.csd.cs.cmu.edu/research/areas/security (last visited Oct. 7, 2015); *About UC Berkeley Security*, UNIV. OF CAL. BERKLEY, http://security.cs.berkeley.edu (last visited Oct. 7, 2015).

[1666] Professor Green's proposed regulatory language reads as follows: "Computer programs and software, a subcategory of literary works, accessible on personal computers and personal devices and protected by technological protection measures ('TPMs') that control access to lawfully obtained works when circumvention is accomplished for the purposes of good faith testing, investigating, or correcting security flaws and vulnerabilities, commentary, criticism, scholarship, or teaching." Green Pet. at 2. Professor Green was represented throughout the rulemaking proceeding by the Samuelson-Glushko Technology Law & Policy Clinic at Colorado Law.

[1667] Bellovin et al.'s proposed regulatory language reads as follows: "Literary works, including computer programs and databases, protected by access control mechanisms that potentially expose the public to risk of harm due to malfunction, security flaws or vulnerabilities when (a) circumvention is accomplished for the purposes of good faith testing for, investigating, or correcting such malfunction, security flaws or vulnerabilities in a technological protection measure or the underlying work it protects; OR (b) circumvention was part of the testing or investigation into a malfunction, security flaw or vulnerability that resulted in the public dissemination of security research when (1) a copyright holder fails to comply with the standards set forth in ISO 29147 and 30111; or (2) the finder of the malfunction, security flaw or

> Proposed Class 25: This proposed class would allow researchers to circumvent access controls in relation to computer programs, databases, and devices for purposes of good-faith testing, identifying, disclosing, and fixing of malfunctions, security flaws, or vulnerabilities.[1668]

In addition to Green and Bellovin et al., comments supporting this class were filed by several other security researchers,[1669] the Internet Association,[1670] Verified Voting Foundation ("VVF"),[1671] the U.S. Public Policy Council of the Association for Computing Machinery ("USACM"),[1672] Free Software Foundation ("FSF"),[1673] Center for Democracy & Technology ("CDT"),[1674] New America's Open Technology Institute ("OTI"),[1675] Rapid7,[1676] Catherine Gellis and the Digital Age Defense project ("Gellis/Digital Age Defense"),[1677] and over 1500 individual commenters.[1678] One party, SAE Vehicle Electrical System Security Committee ("SAE VESS"), submitted a neutral comment, along with an offer to assist the Copyright Office by providing and sharing its technical expertise.[1679]

Second, the Electronic Frontier Foundation ("EFF") filed a petition seeking an exemption to allow the circumvention of TPMs on computer programs that are embedded in motorized land vehicles for purposes of researching the security or safety of that vehicle.[1680] EFF's petition explained that such security and safety research could involve

---

vulnerability reports the malfunction, security flaw or vulnerability to the copyright holder by providing the information set forth in Form A* in advance of or concurrently with public dissemination of the security research." Bellovin et al. Pet. at 1. Professor Andrea Matwyshyn, representing the interests of security researchers and in her capacity as a law professor at Princeton University, later joined Bellovin et al. in their support for the Class 25 exemption, appearing as a witness at the public hearings and submitting a joint response to post-hearing questions.

[1668] NPRM, 79 Fed. Reg. at 73,870.

[1669] Gavin Andersen et al. Supp.; Ian Brown et al. Supp.; Jay Radcliffe Supp.; Mark Stanislav Supp.; Salvatore J. Stolfo Supp.; Brandon Perry Reply; Bruce Schneier Class 25 Reply.

[1670] Internet Association Supp.

[1671] VVF Supp.

[1672] USACM Supp.

[1673] FSF Class 25 Supp.

[1674] CDT Supp.; CDT Reply.

[1675] OTI Class 25 Reply.

[1676] Rapid7 Class 25 Reply.

[1677] Gellis/Digital Age Defense Class 25 Supp.

[1678] Digital Right to Repair Class 25 Supp. (1546 individuals); Brian M. Rice Supp.

[1679] SAE VESS Class 25 Supp.

[1680] EFF's proposed regulatory language reads as follows: "Lawfully-obtained computer programs that control or are intended to control the functioning of a motorized land vehicle, including firmware and firmware updates, where circumvention is undertaken by or on behalf of the lawful owner of such a vehicle for the purpose of researching the security or safety of such vehicles." EFF Vehicle Software Security Pet. at 1.

uncovering errors in software that could cause the car to malfunction or make it vulnerable to remote attacks.[1681] The NPRM described the proposed class as follows:

> Proposed Class 22: This proposed class would allow circumvention of TPMs protecting computer programs that control the functioning of a motorized land vehicle for the purpose of researching the security or safety of such vehicles. Under the exemption as proposed, circumvention would be allowed when undertaken by or on behalf of the lawful owner of the vehicle.

In addition to EFF, comments supporting this class were filed by Professor Green,[1682] FSF,[1683] Gellis/Digital Age Defense,[1684] and over 1800 individual commenters.[1685] Two parties, SAE International Dedicated Short Range Communication Standards Committee ("SAE DSRC") and SAE VESS, submitted neutral comments, along with offers to assist the Copyright Office by providing and sharing their technical expertise.[1686]

Third, the Medical Device Research Coalition ("MDRC"), a group of patients and researchers, filed a petition seeking an exemption to allow the circumvention of TPMs on computer programs on medical devices and their corresponding monitoring systems. MDRC's petition covered two proposed uses—allowing research into software flaws that adversely affect the safety, security and efficacy of medical devices, and allowing a patient to access the information generated by his or her own device.[1687] The Office originally categorized the petition into a single class, described as follows:[1688]

> Proposed Class 27: This proposed class would allow circumvention of TPMs protecting computer programs in medical devices designed for attachment to or implantation in patients and in their corresponding monitoring devices, as well as the outputs generated through those

[1681] *Id.* at 2.

[1682] Green Class 22 Supp.

[1683] FSF Class 22 Supp.

[1684] Gellis/Digital Age Defense Class 22 Supp.

[1685] Digital Right to Repair Class 22 Supp. (1816 individuals); Schneier Class 22 Reply; Donna Eno Class 22 Reply; George Sawyer Class 22 Reply; Louis Wesler Class 22 Reply.

[1686] SAE DSRC Class 22 Supp.; SAE VESS Class 22 Supp.; SAE VESS Class 22 Reply.

[1687] MDRC's proposed regulatory language reads as follows: "Computer programs, in the form of firmware or software, including the outputs generated by those programs, that are contained within or generated by medical devices and their corresponding monitoring systems, when such devices are designed for attachment to or implantation in patients, and where such circumvention is at the direction of a patient seeking access to information generated by his or her own device or at the direction of those conducting research into the safety, security, and effectiveness of such devices." MDRC Pet. at 1-2.

[1688] The Office, however, did ask for comment on "[w]hether the exemption should distinguish among different users (researchers, patients, healthcare providers at the direction of the device-user patient, etc.) and/or the proposed use (examining output of devices, research into safety, security, and effectiveness of devices, etc.)." NPRM, 79 Fed. Reg. at 73,871.

> programs. As proposed, the exemption would be limited to cases where circumvention is at the direction of a patient seeking access to information generated by his or her own device, or at the direction of those conducting research into the safety, security, and effectiveness of such devices. The proposal would cover devices such as pacemakers, implantable cardioverter defibrillators, insulin pumps, and continuous glucose monitors.

In addition to MDRC, comments supporting this class were filed by Professor Green,[1689] Jay Freeman,[1690] Public Knowledge,[1691] FSF,[1692] OTI,[1693] Gellis/Digital Age Defense,[1694] and over 1600 individual commenters.[1695]

Based on the record as it developed in the course of the proceeding, the Register came to the conclusion that Proposed Class 27 should be divided into Proposed Class 27A (Security and Safety Research) and Proposed Class 27B (Patient Data) so that the two distinct purposes can be separately addressed in the Recommendation. The discussion here will focus only on Proposed Class 27A, concerning research into software flaws in medical devices, the analysis of which largely parallels that in Proposed Classes 22 and 25. Proposed Class 27B, which would permit circumvention to allow patient access to information generated by his or her own device, is discussed separately below.

Additionally, as the above makes clear, all three security-related proposals are at some level aimed at allowing security researchers to find flaws in software. Indeed, as one commenter noted, the general software security research exemption in Proposed Class 25 would appear to be broad enough to swallow the more specific exemptions for vehicle software security research in Proposed Class 22 and medical device software security research in Proposed Class 27A.[1696] Given this relationship among the proposed classes, the Register concludes that it is appropriate to consolidate the analysis for these three classes.

The Register further notes that the proposals to some extent referenced circumvention of TPMs protecting "databases."[1697] Databases, however, are distinct

[1689] Green Class 27 Supp.

[1690] Freeman Class 27 Supp.; Freeman Class 27 Reply.

[1691] Public Knowledge Class 27 Supp.; Public Knowledge Class 27 Reply.

[1692] FSF Class 27 Supp.

[1693] OTI Class 27 Reply.

[1694] Gellis/Digital Age Defense Class 27 Supp.

[1695] Digital Right to Repair Class 27 Supp. (1659 individuals); Schneier Class 27 Reply; Don Lowery Class 27 Reply; Gregory Borodiansky Class 27 Reply; Henry Feldman Class 27 Reply; Patrick Ferguson Class 27 Reply; Michael Weinberg Class 27 Reply.

[1696] Green Class 22 Supp. at 1.

[1697] Bellovin et al. Pet. at 1; Green Class 25 Supp. at 4.

from computer programs,[1698] and proponents presented no evidence in the course of the proceeding that demonstrated a need to access databases for purposes of security research. Accordingly, the discussion below excludes databases from consideration.

a. Background

The proponents of the software security exemptions observe as a general matter that software is pervasive in modern machines and devices. They note that software operates the personal computers we use every day, it is the basis of the internet, and it controls increasingly computerized and internet-connected devices such as vehicles, home appliances and medical devices.[1699] In the case of motorized vehicles, computers within the vehicles called electronic control units ("ECUs") monitor and control a variety of vehicle functions.[1700] Similarly, medical devices increasingly employ computers to control and monitor their functions.[1701] The proponents maintain that the security of software and the devices that execute software is of critical importance because security flaws pose potentially serious threats, including physical injury and death, property damage, and financial harm.[1702] Proponents identify a wide variety of TPMs that restrict access to computer software for the proposed uses, including challenge-response mechanisms, dongles, code obfuscation, runtime checks, encryption, and disabled access ports on the circuitry itself.[1703]

Proponents assert that the various types of TPMs and the prohibition against circumvention are having, and will continue to have, an adverse impact on the ability to pursue good-faith research to identify and correct malfunctions, security flaws, and vulnerabilities in computer programs. Although many software developers and device manufacturers conduct their own security research—and sometimes authorize third parties to do the same—the exemptions here are principally aimed at allowing "independent" security researchers who do not have such authorization to engage in the same research without risk of violating the anticircumvention provision of section 1201(a)(1). As discussed below, proponents claim that the permanent statutory exemptions to section 1201(a)(1)'s prohibition—directed to reverse engineering in

[1698] *See* 17 U.S.C. § 101 (defining "computer program" as "a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result"); U.S. COPYRIGHT OFFICE, COMPENDIUM OF U.S. COPYRIGHT OFFICE PRACTICES § 727.1 (3d ed. 2014) ("For purposes of copyright registration, a 'database' is defined as a compilation of digital information comprised of data, information, abstracts, images, maps, music, sound recordings, video, other digitized material, or references to a particular subject or subjects.").

[1699] *See, e.g.*, Bellovin et al. Pet. at 2; Green Class 25 Supp. at 4; EFF Class 22 Pet. at 2-3; MDRC Pet. at 1-2.

[1700] EFF Class 22 Supp. at 2.

[1701] MDRC Supp. at 2.

[1702] *See, e.g.*, Bellovin et al. Pet. at 2; Green Class 25 Supp. at 3-5.

[1703] *See, e.g.*, Green Class 25 Pet. at 2-3; Green Class 25 Supp. at 5-11; Bellovin et al. Pet. at 5; EFF Class 22 Supp. at 4-6; MDRC Supp. at 7-9.

section 1201(f), encryption research in section 1201(g), and security testing in section 1201(j)—do not provide sufficient assurance that the research activities in which they seek to engage will be considered exempt. They therefore seek broader and more flexible exemptions to cover their activities.

In the 2006 anticircumvention exemption proceeding, the Librarian granted a limited exemption for good-faith security research into copy-protected sound recordings on compact discs.[1704] And in the 2010 proceeding, the Librarian granted an exemption for good-faith security research on TPMs protecting video games accessible on personal computers.[1705] The current proposals are significantly broader in scope than what was considered or granted in these prior proceedings.

b. Asserted Noninfringing Uses

Proponents of all three software security research classes assert that accessing and reproducing computer programs for purposes of facilitating good-faith testing for and the identification, disclosure and correction of malfunctions, security flaws and vulnerabilities of computer programs are likely to be noninfringing fair uses under section 107.

In supporting the exemption for vehicle software security research in Proposed Class 22, EFF also invokes section 117 of the Copyright Act, which permits owners of copies of copyrighted computer programs to reproduce and adapt them for certain purposes.[1706]

i. Fair Use

1) Proposed Class 25: Software – Security Research

Class 25 proponents argue that good-faith security research is a noninfringing use because it comprises activities that "either do not constitute copyright infringement or are paradigmatic fair uses."[1707] Proponents identify the following activities as good-faith security research: good-faith testing for, investigation of, and discovery of software flaws and vulnerabilities that implicate privacy, security, and safety concerns; alerting consumers and companies to the existence of such flaws and vulnerabilities; teaching students and providing them with hands-on experience investigating real systems and devices; publicizing scientific findings related to the investigation of software flaws and vulnerabilities through academic publications, conference presentations, and other discussions of software and device security; and applying research discoveries to correct

[1704] 2006 Final Rule, 71 Fed. Reg. at 68,477.

[1705] 2010 Final Rule, 75 Fed. Reg. at 43,832-33.

[1706] EFF Class 22 Supp. at 12-16.

[1707] *See, e.g.*, Green Pet. at 3; Green Class 25 Supp. at 11; Green Class 25 Reply at 6; *see also* Bellovin et al. Pet. at 2; CDT Reply at 4.

vulnerabilities and create better functioning and more secure software.[1708] Proponents urge that unlike the 2006 and 2010 exemptions that were limited to vulnerabilities caused by access controls themselves, the currently requested exemption should cover all software that might contain vulnerabilities—not just access controls—because "the landscape of security vulnerabilities has changed" to encompass both vulnerabilities in TPMs themselves as well as in underlying computer programs.[1709]

Proponents point to a variety of devices and computer code that would be the focus of their research. By and large, these examples involve software and devices used by individual consumers. For example, proponents note potential issues with internet-enabled consumer goods, such as webcams and microphones on computers, internet-connected smoke alarms, carbon monoxide detectors, and security cameras.[1710] At the public hearing, one proponent highlighted a flaw in a Wi-Fi-enabled voicemail device designed for children that could allow hackers to access information stored on the device and leave their own messages.[1711] Proponents cite research on automobiles that has revealed vulnerabilities in remote unlocking functions and wireless tire pressure monitoring systems.[1712] Proponents also express the desire to research voting machines to find flaws in the underlying code and in the encryption protecting it, which could potentially allow alteration of votes.[1713] Although, in their petition, Bellovin et al. also mention the possibility of researching "computer code that controls nuclear power plants, smartgrids, and industrial control systems" as well as "the computer code in air traffic

[1708] Bellovin et al. Pet. at 2; Green Class 25 Supp. at 11-14; *see also* Bellovin et al. Supp. at 4; USACM Supp. at 1; Stolfo Supp. at 1; VVF Supp. at 1; FSF Class 25 Supp. at 1; Internet Association Supp. at 1; Radcliffe Supp. at 1; Stanislav Supp. at 1; OTI Class 25 Reply at 5; Rapid7 Reply at 1; Tr. at 10:14-17 (May 26, 2015) (Green); Tr. at 31:15-23 (May 26, 2015) (Reid on behalf of Green); Tr. at 49:06-10 (May 26, 2015) (Bellovin).

[1709] Green Class 25 Reply at 11; *see also* CDT Reply at 4-6 (asserting that security research is a noninfringing fair use regardless of whether it is on a TPM or a work protected by that TPM).

[1710] Bellovin et al. Supp. at 9; Green Class 25 Supp. at 11-12. Class 25 proponents also refer in passing to medical devices in some of their submissions. *See, e.g.*, Bellovin et al. Pet. at 3 (asserting that adverse effects, such as death or physical harm, can result from malfunctions, security flaws, or vulnerabilities in "medical devices and machines including radiation machines"); CDT Reply at App. A at 3 (noting that researchers have found flaws in "pharmaceutical drug compounders, automated external defibrillators, ventilators, drug infusion pumps, and implantable medical devices"). Class 27A, however, specifically addresses partially or wholly implanted medical devices, and Class 25 proponents did not provide any specific evidence supporting a need to circumvent non-implanted medical devices.

[1711] Tr. at 41:03-08 (May 26, 2015) (Stanislav, Rapid7).

[1712] Bellovin et al. Supp. at 4-7; Tr. at 164:20-24 (May 26, 2015) (Moy, OTI); Tr. at 194:02-05 (May 26, 2015) (Bellovin).

[1713] VVF Supp. at 1; Tr. at 72:11-20 (May 26, 2015) (Blaze).

control systems, train systems and traffic lights,"[1714] their later submissions do not focus on these activities and instead highlight consumer-oriented software and products.[1715]

Proponents contend that security research does not constitute copyright infringement because, as Green states, "[t]he vast majority of computer security research . . . simply involves accessing functional, non-copyrighted elements of the works," such as a computer program's object code.[1716] Green further asserts that "in most security research, nothing is reproduced, distributed, or adapted" and that at most, there is "incidental reproduction, distribution, or adaptation . . . ancillary to the research."[1717]

Even where there is more than *de minimis* reproduction, distribution, or adaptation, proponents argue such security research is "universally likely to be a non-infringing fair use."[1718] Proponents assert that the first factor, the purpose and character of the use, weighs strongly in favor of fair use because the purposes of security research—specifically, investigating and discovering security flaws, documenting and disclosing security flaws to companies and the public, and allowing students to investigate software in classroom labs—all fall within the "paradigmatic fair uses" listed in section 107's preamble. They contend that security research is transformative since it "accomplishes a wholly different purpose than that served by the original work."[1719]

According to proponents, the second factor, the nature of the copyrighted work, also weighs in favor of fair use because security research is focused on computer programs, which are "more factual and functional than they are creative" and "embody many functional design elements that copyright law does not protect."[1720] As for the third factor, the amount and substantiality of the use, proponents contend that it carries little weight because security researchers "often utilize few or none of a piece of software's copyrighted elements," and even when such elements are used, it is in a way that is "merely incidental to the goal of the research."[1721] They also note that publication

[1714] Bellovin et al. Pet. at 2.

[1715] *See* Bellovin et al. Supp. at 9-10 (mentioning research into security vulnerabilities in "popular consumer programs," "cars," "Internet of Things products" such as smoke alarms and carbon monoxide detectors, "surveillance cameras," "card payment systems, and mobile payment platforms," "'smart' locks, safes and vaults and alarm systems," "electronic voting systems," and "medical devices").

[1716] Green Class 25 Supp. at 14.

[1717] *Id.* at 15.

[1718] *Id.*; *see also* Green Class 25 Reply at 8; CDT Reply at 4.

[1719] CDT Reply at 4; *see also* Green Class 25 Supp. at 15-16; Green Class 25 Reply at 8.

[1720] Green Class 25 Supp. at 16; *see also* CDT Reply at 4-5 (quoting 2010 Recommendation at 184-85); Green Class 25 Reply at 8.

[1721] Green Class 25 Supp. at 16-17; *see also* CDT Reply at 5 (asserting that "the reproduction of the expressive elements of a protected work in security research results is likely to be small, limited to the part of the software that makes the system vulnerable to cyberattack"); Green Class 25 Reply at 8.

of such research utilizes little of the original work and does so in a way that is transformative.[1722]

Finally, proponents argue that the fourth factor, the effect on the potential market for or value of the work, weighs in favor of fair use as well because security research "will not usurp the market for any original works subject to said research," particularly because good-faith security researchers have to lawfully obtain a copy of the work in order to conduct security research on the work. Proponents further assert that any economic or reputational harm resulting from the disclosure of security flaws or vulnerabilities is not a relevant consideration and, in any event, is "likely [to] be avoided through coordinated disclosure with the company." [1723] Finally, they point out that when research fails to discover vulnerabilities and instead confirms the security of the work, this will only enhance the work's value.[1724]

Proponents also argue that previously granted exemptions in 2006 and 2010 that were relevant to security research "demonstrate the widespread understanding that good faith security research is a non-infringing use."[1725] Although, as noted above, they do not seek to rely on any of the permanent security-related exemptions in section 1201, proponents nonetheless assert that "Congress has implicitly recognized security research as a non-infringing use by codifying statutory support for reverse engineering, encryption research, and security testing in Section 1201(f), (g), and (j)." According to proponents, those subsections would be "meaningless if the underlying acts of reverse engineering, encryption research, and security testing were treated as copyright infringement."[1726] Bellovin et al. further assert that section 1201(i), which allows individuals to circumvent TPMs that collect personally identifying information,[1727] also demonstrates security research to be a noninfringing use because it shows that "Congress specifically contemplated and sought to protect the public from malfunctioning, flawed or vulnerable code that harms consumers."[1728]

[1722] *Id.*

[1723] Green Class 25 Supp. at 17; CDT Reply at 5-6 (quoting 2010 Recommendation at 186); *see also* Green Class 25 Reply at 9.

[1724] *Id.*

[1725] Green Class 25 Reply at 7; *see also* Bellovin et al. Supp. at 4-5; Bellovin et al. Pet. at 2; CDT Supp. at 2 (citing 2010 Final Rule, 75 Fed. Reg. at 43,833); CDT Reply at 4, 6 (finding that security research, regardless of whether it is on a TPM or a work protected by that TPM, is a noninfringing fair use because "[t]he Copyright Office has . . . concluded that such research is fair use").

[1726] Green Class 25 Reply at 7; *see also* Bellovin et al. Supp. at 4.

[1727] 17 U.S.C. § 1201(i).

[1728] Bellovin et al. Supp. at 5; *see also* Tr. at 70:04-21 (May 26, 2015) (Matwyshyn).

2) Proposed Class 22: Vehicle Software – Security and Safety Research

Class 22 proponents note that the ECUs of modern motorized land vehicles (a category that includes personal automobiles, commercial vehicles, and farm equipment) control a wide array of critical functions including ignition, braking, and engine power.[1729] Proponent EFF thus states that "[f]or vehicles to remain safe and secure, it is essential that users be able to study the software that controls vehicular computers" so that "[i]ndependent researchers can discover programming errors that endanger passengers."[1730] For instance, EFF notes that such errors led to an "unintended acceleration defect that caused a fatal accident."[1731] It explains that "[i]ndependent researchers have also found errors that would allow a remote attacker to take control of a vehicle's functions, and have written a patch to resolve the vulnerability."[1732]

Proponents assert that their proposed research activities constitute noninfringing fair use. For purposes of the first fair use factor, EFF maintains that the proposed uses of vehicle software for research and scholarship "are purposes that are explicitly called out in Section 107 as supporting a finding of fair use."[1733] EFF contends that security research serves new and transformative purposes.[1734] It further asserts that case law demonstrates that uses enabling "greater access to information," such as copying software in order to understand and analyze its functions, are fair uses.[1735] EFF also notes that the Register found in 2010 that "good faith research constitutes fair use" and recommended an exemption allowing security research for video games, arguing that the proposed exemption is "comparable" to the 2010 exemption.[1736] EFF explains that security researchers are more interested in the functional aspects rather than the creative, copyrightable elements of vehicle software since vulnerabilities and errors lie in a code's functionality.[1737] It further asserts that security research has socially beneficial purposes that weigh "heavily in favor of fair use" because the research results in public scrutiny that incentivizes manufacturers to more carefully program vehicles and fix known flaws.[1738]

[1729] EFF Class 22 Supp. at 2.

[1730] *Id.*

[1731] *Id.*

[1732] *Id.*

[1733] *Id.* at 7.

[1734] *Id.* at 7-11 (citing *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 579 (1994)).

[1735] *See id.* at 7-8 (citing *Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1522-23 (9th Cir. 1992)); EFF Class 22 Reply at 4-5.

[1736] EFF Class 22 Supp. at 8 (quoting 2010 Final Rule, 75 Fed. Reg. at 43,834).

[1737] *Id.* at 8-9.

[1738] *Id.* at 9-10.

Turning to the second fair use factor, EFF states that the nature of the computer programs on vehicle ECUs weighs heavily in favor of fair use because the code contains "'unprotected aspects that cannot be examined without copying.'"[1739] EFF also asserts that "[t]he primary significance, and nature, of vehicle firmware is functional, strongly favoring fair use."[1740]

With regard to the third factor, the amount of the copyrighted work used, EFF recognizes that the entire work may be used.[1741] But it explains that this does not preclude a finding of fair use. EFF observes that the relevant analysis includes a consideration of whether the quantity and value of the materials used are reasonable in relation to the purpose of the copying.[1742] EFF asserts that in the case of vehicle security and safety research, copying of computer programs on ECUs will be limited to that which is reasonable and for a legitimate purpose.[1743]

Finally, EFF asserts that the fourth factor, the effect on the market for or value of the copyrighted work, also favors fair use.[1744] EFF notes that there is no market for computer programs on ECUs apart from the sale of vehicles themselves, and so the uses encompassed by the proposed exemption, by definition, cannot substitute for sales of the vehicle software.[1745] EFF also maintains that the relevant harm for consideration is the harm to the market for the copyrighted works themselves, not harms resulting from non-copyright issues, such as concerns that allowing researchers to investigate software flaws could raise public safety issues, or adversely affect vehicles' compliance with safety or emissions regulations.[1746] EFF thus rejects as inapposite opponents' claims regarding market effects resulting from such "non-copyright issues."[1747]

3) Proposed Class 27A: Medical Device Software – Security and Safety Research

Class 27A proponents seek to access the computer code of medical devices and corresponding monitoring systems and "use this information to analyze the safety and

---

[1739] *See, e.g.*, *id.* at 10 (quoting *Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596, 603 (9th Cir. 2000)).

[1740] *Id.*

[1741] *Id.*

[1742] *Id.* (citing *Campbell*, 510 U.S. at 586-87); EFF Class 22 Reply at 7 (citing *Kelly v. Arriba Soft Corp.*, 336 F.3d 811, 820-21 (9th Cir. 2002) and *Mattel, Inc. v. Walking Mountain Prod.*, 353 F.3d 792, 803 n.8 (9th Cir. 2003)).

[1743] EFF Class 22 Supp. at 10-11; EFF Class 22 Reply at 7.

[1744] *See, e.g.*, EFF Class 22 Supp. at 11 (again likening the proposed exemption to the 2010 video game exemption); EFF Class 22 Reply at 7-8.

[1745] EFF Class 22 Supp. at 11.

[1746] EFF Class 22 Reply at 7-8.

[1747] *Id.*

performance of these devices."[1748] MDRC explains that by "medical devices," it means, specifically, "devices that are physically implanted in whole or in part to the body and are used as part of the delivery of therapy and medical care to a patient," including pacemakers, ICDs, insulin pumps, and continuous glucose monitors.[1749] While in its petition MDRC also referred to "devices [that] are designed for attachment" as well as implantation in patients,[1750] MDRC's subsequent filings and the remainder of the record demonstrate that the proposed exemption is not intended to encompass attached devices that are neither wholly nor partially implanted, and MDRC specifically excludes "consumer health devices, such as digital pedometers and other devices that gather data and report their results directly to the patient."[1751] The term "[c]orresponding monitoring systems," in turn, refers to devices such as handheld receivers or monitoring base stations that wirelessly receive data from medical devices, and in some cases further relay that data to a centralized monitoring facility or to the physician.[1752] As used herein, then, the term "corresponding" or "personal" monitoring system means a portable or home monitoring system rather than a monitoring system that resides at a centralized facility or with a health care provider.[1753]

Proponents assert that under the four-factor fair use analysis, independent researchers are entitled to research medical device software for flaws that affect the safety, security, or effectiveness of those devices.[1754] As an overarching point, MDRC

[1748] MDRC Supp. at 2.

[1749] *Id.* Pacemakers and ICDs are wholly implanted within the body, usually in the chest or the abdomen. *See* Daniel Halperin et al., *Security and Privacy for Implantable Medical Devices*, 7 IEEE: PERVASIVE COMPUTING 30, 32 (2008), https://spqr.eecs.umich.edu/papers/b1kohFINAL2.pdf (cited in MDRC Supp. at 2 n.4); NAT'L HEART, LUNG, AND BLOOD INST., *What Is an Implantable Cardioverter Defibrillator?*, NAT'L INST. OF HEALTH, http://www.nhlbi.nih.gov/health/health-topics/topics/icd (last visited Oct. 7, 2015) (cited in MDRC Supp. at App. C at ¶ 5 n.12). Insulin pumps, which consist of needles and tubing attached to the body that deliver insulin doses, and continuous glucose monitors, which consist of sensors placed under the skin, are only partially implanted, and can be described as temporary, as they often require replacement after a set period of days. *See* Jerome Radcliffe, *Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System*, BLACK HAT (2011), https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf (cited in MDRC Supp. at 10 n.62); Tr. at 8:10-19 (May 29, 2015) (West, MDRC).

[1750] MDRC Pet. at 1.

[1751] MDRC Supp. at 2 n.4.

[1752] *Id.* at 5, 7-8, App. C; *see also* Tr. at 8:10-19 (May 29, 2015) (West, MDRC); Tr. at 53:10-14 (May 29, 2015) (Sellars, MDRC); Sherwin Siy, *Copyright Law and My Mother's Heart*, PUBLIC KNOWLEDGE (Jan. 20, 2015), https://www.publicknowledge.org/news-blog/blogs/copyright-law-and-my-mothers-heart (cited in MDRC Supp. at 11 n.68) (noting that data from a pacemaker and emergency defibrillator "are stored on the device itself," then "transferred to the base station, and then later transmitted to a monitoring company," which will notify the doctor of any pertinent information, or that alternatively data can be retrieved through direct interrogations by a doctor).

[1753] *See* MDRC Supp. at App. C; Tr. at 48:02-09 (May 29, 2015) (Sellars, MDRC).

[1754] *See, e.g.*, MDRC Supp. at 10-14; MDRC Reply at 20-22; Public Knowledge Class 27 Reply at 3; Public Knowledge Class 27 Supp. at 2. For the purposes of the Class 27A analysis conducted herein, the term "medical devices" refers to networked computerized medical devices that may employ computer programs.

observes with respect to security issues that "[t]o the extent that researchers . . . implicate [the exclusive rights of copyright owners], it is usually in the context of short quotations from the code or data outputs of a device included in a final report analyzing the device, or through the creation of intermediate, in-house copies of the code or outputs while the researcher is in the process of analyzing the work."[1755] With respect to any such interim copies of medical device computer programs, proponents contend that these constitute fair use.[1756] Concerning the use of quoted segments of computer programs, MDRC contends under the first factor that independent researchers' use of such segments in publications detailing their findings is for a transformative purpose, because it "adds to the original with a new meaning or message."[1757] MDRC also contends that publication of research findings "is also often . . . done for non-commercial, educational purposes, often at academic institutions."[1758]

As for the second fair use factor, MDRC asserts that the nature of the work weighs in favor of fair use, because the medical device computer programs at issue are highly utilitarian.[1759] Turning to the third fair use factor, MDRC maintains that the relatively small amount of medical device code that is used by independent researchers in publications of their findings weighs in favor of fair use, because the computer program "can be tens of thousands of lines long, and has no identifiable 'heart.'"[1760] Even where interim copies of the whole work need to be made, MDRC points to case law holding that making such copies "to access the unprotectable functional elements of software is a fair use."[1761] MDRC also stresses that independent security researchers make interim copies for a transformative purpose, namely, "producing analysis into the safety and effectiveness of devices" and not to "develop[] complementary or rival software."[1762]

MDRC contends the fourth fair use factor, the effect of the use on the potential market for or value of the work, also weighs in favor of using medical device code in published findings.[1763] Specifically, it asserts that independent researchers' excerpting of

---

The copyrighted work is generally referred to as "medical device software." The terms medical device "users" and "patients" are also used interchangeably.

[1755] MDRC Supp. at 11.

[1756] *Id.* at 13-15; Public Knowledge Class 27 Supp. at 2. Public Knowledge alternatively suggests, without offering specific factual support, that the copies fail to meet the statutory definition of a "reproduction" as *de minimis* copies. Public Knowledge Class 27 Supp. at 2.

[1757] MDRC Supp. at 11-12 (citing *Campbell*, 510 U.S. at 579).

[1758] *Id.* at 11.

[1759] *Id.* at 12 (citing *Connectix*, 203 F.3d at 603).

[1760] *Id.* (citing *Medical Device Software Validation*, MATHWORKS, http://www.mathworks.com/solutions/medical-devices/medical-software-validation.html (last visited Oct. 7, 2015) and *Harper & Row Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 565 (1985)).

[1761] *Id.* at 13 (citing *Connectix*, 203 F.3d at 608.

[1762] *Id.* at 14.

[1763] *Id.* at 12-13.

medical device code in such a context does not usurp market demand for the medical device itself.[1764] Similarly, it argues that the making of interim copies made in the process of conducting research "could not possibly supplant the need for an original device in a patient."[1765] Moreover, MDRC asserts that any market harm resulting from such uses "would only be due to the effectiveness of its criticism, which is not considered cognizable harm under the fourth factor."[1766]

ii. Section 117

1) Proposed Class 22: Vehicle Software – Security and Safety Research

With regard to Class 22, in addition to relying on fair use, EFF asserts that, vehicle owners' access, reproduction or alteration of vehicle computer programs for security research is a noninfringing use under section 117. That provision allows the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that program "as an essential step in the utilization of the computer program in conjunction with a machine and that [] is used in no other manner."[1767]

A key consideration with respect to the application of section 117 is who owns the computer program in question. EFF argues that under either of the two leading cases on software ownership—*Krause v. Titleserv, Inc.*[1768] and *Vernor v. Autodesk, Inc.*[1769]—it is the owner of the vehicle who owns the copy of the computer programs on an ECU embedded in the owner's vehicle.[1770] EFF states that most vehicle ECUs are transferred as part of the vehicle with no explicit agreement governing title to the copies of the ECU computer programs.[1771] EFF noted during the initial round of comments that it was able to identify only a few license agreements pertaining to ECUs, and that these addressed vehicle telematics systems[1772] or entertainment systems; it did not locate any concerning more general vehicle functions.[1773] And, during the reply phase, EFF noted that

---

[1764] *Id.* at 12 (citing *Cariou v. Prince*, 714 F.3d 694, 708-09 (2d Cir. 2013)).

[1765] *Id.* at 14.

[1766] *Id.* at 12 (citing *New Era Publ'ns Int'l v. Carol Publ'g Grp*., 904 F.2d 152, 160 (2d Cir. 1990); *Wojnarowicz v. Am. Family Ass'n*, 745 F. Supp. 130, 145-46 (S.D.N.Y. 1990); 2012 Recommendation at 73).

[1767] 17 U.S.C. § 117(a).

[1768] 402 F.3d 119 (2d Cir. 2005).

[1769] 621 F.3d 1102 (9th Cir. 2010).

[1770] *See, e.g.*, EFF Class 22 Supp. at 12-15; EFF Class 22 Reply at 8-10.

[1771] EFF Class 22 Supp. at 13.

[1772] Telematics systems are vehicle systems that combine global positioning satellite tracking and other wireless communications to identify the location of vehicles for a variety of purposes such as automatic roadside assistance. *See id.* at 14.

[1773] *Id.* at 13-14 (citing end-user license agreements for GM OnStar, Pioneer AppRadioLIVE, Ford Sync, Toyota Safety Connect, and Mercedes-Benz mbrace).

opponents had failed to offer any additional evidence that the copies of computer programs on ECUs are licensed rather than sold to vehicle purchasers.[1774]

EFF further maintains that even if written license terms exist, under relevant precedent, a vehicle owner may still own the copy of computer programs on an ECU in his or her car. EFF further asserts that under *Krause* and *Vernor*, possessing title to a software copy is not an "absolute prerequisite" to section 117(a) protection.[1775] Rather, a party who exercises sufficient incidents of ownership over a copy of the program can be considered the owner of it.[1776] EFF claims that such incidents of ownership exist for vehicle purchasers, noting that vehicle owners are understood to have the right to indefinitely use, possess, resell, discard or destroy their vehicles, including the embedded ECUs, without any material restriction from the manufacturer.[1777]

EFF additionally asserts that making copies or adaptations of ECU computer programs for the desired uses is "an essential step in the utilization of the computer program in conjunction with a machine and that [the copy or adaptation] is used in no other manner," as required to invoke section 117.[1778] Although EFF concedes that making such copies and adaptations may not be essential to using the vehicle as intended by the manufacturer, relying upon *Krause*, it stresses that section 117 allows the making of such copies and adaptations for the purpose of adding new features and capabilities, which could include the testing of bug fixes.[1779] Additionally, EFF maintains that the creation of a backup copy to protect against destruction of or damage to the ECU software in the process of vehicle software security research is covered by the archival purposes exception set forth in section 117(a)(2), which permits the making of "a new copy or adaptation . . . for archival purposes only" so long as "all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful."[1780] EFF notes that such backup copies "serve as a reference when modifications or experimentations are performed" and can be used to restore the ECU to its original state after completing research on the vehicle.[1781]

[1774] EFF Class 22 Reply at 9-10.

[1775] EFF Class 22 Supp. at 12-14 (citing *Krause*, 402 F.3d at 124 and *Vernor*, 621 F.3d at 1110-11).

[1776] EFF Class 22 Reply at 9.

[1777] *Id.* at 9-10.

[1778] EFF Class 22 Supp. at 15.

[1779] *Id.* (citing *Krause*, 402 F.3d at 127).

[1780] *Id.* at 15-16; EFF Class 22 Reply at 10-11.

[1781] EFF Class 22 Reply at 10-11.

c. Asserted Adverse Effects

i. Proposed Class 25: Software – Security Research

Class 25 proponents argue that an exemption is necessary because section 1201(a)(1) has "significant chilling effects on good faith security research" in that it can potentially expose security researchers to significant civil and criminal liability.[1782] Green highlights one example in which a copyright owner, the Secure Digital Music Initiative, publicly challenged security researchers from Princeton, Rice, and Xerox to find vulnerabilities in technologies protecting digital music, then subsequently sent letters threatening to bring lawsuits against those who succeeded in removing the protections and intended to present their results at an academic conference.[1783] Green provides a second example where researchers discovered vulnerabilities in "the Texas Instruments' Data Storage Tag[], which uses sensors to track information."[1784] According to Green, "Texas Instruments contacted officials at the researchers' universities in an attempt to block disclosure," although he acknowledges that "[t]hese attempts were ultimately unsuccessful."[1785] Proponents also contend that foreign security researchers, such as those from Russia and the United Kingdom, have been deterred from working in and traveling to the United States "for fear of prosecution under the anti-circumvention provision."[1786]

Supporters of Proposed Class 25 comment that the DMCA gives the "bad-guy" researchers an advantage because it chills "good-guy" researchers who are focused on making the public safer.[1787] CDT asserts that the DMCA's anticircumvention rule "discourages both academic institutions and government entities from funding critical security research."[1788] Proponents also argue that the prohibition on circumvention has resulted in lower-quality research, because researchers alter the subject matter and methodology of the intended research to avoid violating section 1201(a)(1). Bellovin et al. explain that this loss of security research has harmed "not only our own national

---

[1782] Green Class 25 Supp. at 17-18; *see also* CDT Supp. at 3; Radcliffe Class 25 Supp. at 1; Rice Class 25 Supp. at 1; Stanislav Class 25 Supp. at 1; USACM Supp. at 1; Green Class 25 Reply at 4; Tr. at 20:08-23 (May 26, 2015) (Green); Tr. at 38:01-20 (May 26, 2015) (Sayler on behalf of Green); Tr. at 40:24-42:04 (May 26, 2015) (Stanislav, Rapid7); Tr. at 71:01-08 (May 26, 2015) (Matwyshyn). As explained by Green, researchers can face civil damages "up to $2,500 per act of circumvention" and criminal penalties of "up to $500,000, up to 5 years in prison, or both," and any subsequent violation can result in "a fine of up to $1 million, 10 years in prison, or both." Green Class 25 Supp. at 18.

[1783] Green Class 25 Supp. at 18.

[1784] *Id.*

[1785] *Id.*

[1786] *Id.* at 19; *see also* Brown et al. Class 25 Supp. at 1 (contending that the prohibition on circumvention "significantly damages international collaboration in computer security research").

[1787] Radcliffe Supp. at 1; *see also* Schneier Class 25 Reply at 2; OTI Class 25 Reply at 2-5; Tr. at 96:10-97:07 (May 26, 2015) (Moy, OTI).

[1788] CDT Reply at 6.

security but also the security of other countries," as well as consumer safety, by impeding the diagnosis and mitigation of defects in consumer products.[1789] Bellovin et al. also argue that the lack of an exemption interferes with educational initiatives relating to security research.[1790]

Proponents also reject opponents' argument, described in greater detail below, that an exemption is unnecessary because software companies and system and device manufacturers work with outside security researchers in authorized settings. Proponents assert that such efforts are often not productive because the authorizing company may decide not to disclose or resolve any discovered vulnerabilities.[1791] Bellovin et al. further express concerns that arrangements between companies and security researchers may give the companies the right to block or delay publication or other disclosure of vulnerabilities, thereby chilling security researchers' desire to enter into such arrangements.[1792] For example, Professor Bellovin testified at the public hearing that his university's ethics policies prohibit him from "accept[ing] a grant that gives the funding agency or some outside party the right to block publication."[1793] CDT worries that relying on agreements between companies and researchers does not provide "protection for independent or 'accidental' researchers who discover a vulnerability but have no means to disclose it without potentially subjecting themselves to liability under Section 1201."[1794]

As noted above, proponents' evidence focused largely on the adverse effects flowing from the inability to research software and devices that are intended for use by individual consumers. They cite as examples internet-connected consumer devices such as webcams, smoke alarms, alarm systems, security cameras, card payment systems and mobile payment platforms used by individual consumers.[1795] They also point to voting machines, which have previously been found to have "serious exploitable vulnerabilities . . . that could be used to undetectably alter the outcome of an election."[1796] Proponents did not specifically address how the prohibition on circumvention is adversely affecting security research into computer programs that control non-consumer-facing systems such as those used to operate nuclear power plants, smartgrids, industrial enterprises, air traffic

[1789] Bellovin et al. Supp. at 7; *see also* Brown et al. Class 25 Supp. at 1 (asserting that the prohibition on circumvention "materially harms matters of national security in both the US and UK"); FSF Class 25 Supp. at 1; Stolfo Class 25 Supp. at 1 (stating that the DMCA has caused Stolfo to "alter and, in my opinion, methodologically weaken the proposals that I have submitted to government funding agencies in response to their calls for security research"); USACM Supp. at 1.

[1790] Bellovin et al. Class 25 Supp. at 7; *see also* Stolfo Supp. at 1.

[1791] CDT Reply at 7-8; *see also* Schneier Class 25 at 1-2.

[1792] Tr. at 204:21-205:09 (May 26, 2015) (Bellovin).

[1793] *Id.* at 159:06-160:22 (Bellovin).

[1794] CDT Reply at 8.

[1795] Bellovin et al. Supp. at 9-10.

[1796] *Id.* at 2-3.

control functions, train systems, or traffic lights,[1797] or explain why that research could not or should not be conducted under the authorization of the relevant system owner.

While Class 25 proponents acknowledge that section 1201 contains a number of potentially relevant permanent exemptions—section 1201(f) for reverse engineering, section 1201(g) for encryption research, and section 1201(j) for security testing—they nevertheless claim these exemptions are inadequate because they have "overly narrow scopes, restrictions on research, restrictions on dissemination of information, authorization requirements, reliance on multifactor tests, and other infirmities" and lack the clarity and breadth necessary to facilitate researchers' desired activities.[1798] Green notes that the Register recommended a security research exemption for copy-protection controls on compact discs in 2006, and one for TPM-protected video games in 2010, where the applicability of section 1201's permanent exemptions was inadequate and needed to be supplemented to better facilitate important research.[1799]

The reverse engineering exemption in section 1201(f) permits circumvention for the purpose of identifying and analyzing elements of computer programs necessary to achieve interoperability and allow development of circumvention methods to enable such analysis and the interoperability of independently created computer programs.[1800] According to Green, that provision does not obviate the need for the proposed exemption here because "not all vital security research has the 'sole purpose' of improving interoperability," as required under 1201(f).[1801] Green notes that research may have other purposes as well, such as exposing security flaws, incentivizing repair of flaws, and teaching students how to conduct security research.[1802]

The encryption research exemption in section 1201(g) is intended to allow for the research of and advancement of encryption technologies. Green argues that this provision is also insufficient.[1803] For example, section 1201(g) is limited to the purposes of advancing the state of knowledge in the field of encryption technology or assisting in the development of encryption products.[1804] Proponents note that security research does

---

[1797] *See* Bellovin et al. Pet. at 2.

[1798] Green Class 25 Supp. at 19; *see also* CDT Supp. at 3-4; Green Class 25 Reply at 9; Tr. at 14:16-25, 17:13-19 (May 26, 2015) (Reid on behalf of Green).

[1799] Green Class 25 Reply at 9-10; Tr. at 15:22-16:10 (Reid on behalf of Green). Proponents argue that while the permanent exemptions do reflect Congress's intent to allow security testing, the fact that targeted exemptions have been previously granted in the realm of security research demonstrates the need for a targeted exemption here. Green Class 25 Reply at 10-11; *see also* Tr. at 113:11-23 (May 26, 2015) (Stallman, CDT).

[1800] 17 U.S.C. § 1201(f).

[1801] Green Class 25 Supp. at 19-20.

[1802] *Id.*

[1803] *Id.* at 20-21.

[1804] 17 U.S.C. § 1201(g).

not always involve encryption technologies.[1805] For instance, Bellovin et al. list a number of categories of security flaws, only some of which involve encryption.[1806] Moreover, the 1201(g) exemption requires researchers to attempt to obtain authorization from copyright holders;[1807] proponents assert that in some cases copyright owners who learn about planned research attempt to squash it by threatening spurious legal action.[1808] Green also contends that section 1201(g) requires the evaluation of a multifactor statutory test that is restrictive, somewhat vague in its application to both professional and amateur security researchers, and difficult to apply *ex ante*.[1809]

The security testing exemption in section 1201(j) authorizes accessing a computer system or network for the purpose of testing, investigating, or correcting flaws or vulnerabilities.[1810] Proponents assert that this provision is restrictive and is difficult to apply.[1811] Proponents contend that the language requiring that testing be of "a computer, computer system, or computer network" makes it unclear whether the exemption applies when a researcher "is not seeking to gain access to 'a computer, computer system, or computer network,'" but is attempting to research flaws in software.[1812] Section 1201(j) also requires that the testing be "with the authorization of the owner or operator of such computer, computer system, or computer network."[1813] Proponents contend that it may be difficult to know who "the owner or operator" of a system is, particularly when testing software that is used in a range of devices, and that, in any event, authorization can be unreasonably withheld.[1814] CDT further observes that 1201(j) does not make provision for the "accidental researcher," a person who simply discovers a vulnerability while in the midst of "wholly separate research."[1815]

Proponents also complain that the multifactor test set forth in section 1201(j) is difficult to apply *ex ante* and has requirements that are not practical for security researchers. For example, while the multifactor test requires consideration of whether the activity is "solely for the benefit of a computer's owner or operator," some research may

[1805] Green Class 25 Supp. at 20.

[1806] Bellovin et al. Supp. at 5 (listing, for example, "[p]assive interception of communication," "[c]ode injection through mechanisms such as buffer/heap/stack overflows," and "[r]ootkits" as well as "[w]eaknesses in . . . cryptographic practices").

[1807] 17 U.S.C. § 1201(g)(2)(C) (requiring the person to have "made a good faith effort to obtain authorization before the circumvention").

[1808] Green Class 25 Supp. at 20.

[1809] *Id.* at 21.

[1810] 17 U.S.C. § 1201(j).

[1811] Green Class 25 Supp. at 21-22; CDT Supp. at 3-4; CDT Reply at 8.

[1812] Green Class 25 Supp. at 21 (citing 2010 Final Rule, 75 Fed. Reg. at 43,832-33).

[1813] 17 U.S.C. § 1201(j)(1).

[1814] Green Class 25 Supp. at 21-22; CDT Supp. at 3-4; CDT Reply at 8; Tr. at 101:03-12 (May 26, 2015) (Stallman, CDT); Tr. at 117:04-22 (May 26, 2015) (Reid on behalf of Green).

[1815] Tr. at 107:07-25 (May 26, 2015) (Stallman, CDT).

result in "outcomes that . . . benefit the public" rather than the owner or operator.[1816] CDT also argues that the requirement in 1201(j) that an act of circumvention not violate "applicable law other than this section" only "imports ambiguities" from other statutes, including the Computer Fraud and Abuse Act ("CFAA").[1817] The CFAA is expressly referenced in section 1201(j)[1818] and, as most relevant here, prohibits the act of intentionally accessing a "protected" computer (defined as any federal computer, bank computer, or computer connected to the internet) without authorization to obtain information, commit fraud or theft, or damage the computer.[1819]

Proponents assert that there are no reasonable alternatives to circumvention that exist for security research because "all instances of the software or device under investigation are protected by TPMs."[1820] In addition, they claim that "software developers and copyright holders lack adequate incentives to conduct the necessary security research themselves" and may instead attempt to conceal security vulnerabilities.[1821]

ii. Proposed Class 22: Vehicle Software – Security and Safety Research

Regarding Class 22, EFF posits that it is essential for independent researchers "to study the software that controls vehicular computers" in order to ensure public safety and security.[1822] EFF asserts that manufacturers' efforts are insufficient on their own to address the security and safety concerns posed by vehicle software.[1823] EFF observes

[1816] Green Class 25 Supp. at 22; *see also* CDT Reply at 9 (asserting that "with the proliferation of software-enabled or networked devices, the person whose property, safety, or privacy is protected by the lock may not be able to authorize testing it"); Tr. at 14:25-15:12 (May 26, 2015) (Reid on behalf of Green).

[1817] *See* CDT Reply at 8-9; Tr. at 121:18-122:24 (May 26, 2015).

[1818] 17 U.S.C. § 1201(j).

[1819] 18 U.S.C. § 1030. Proponents also complain about ambiguities in other potentially relevant statutes, including the Wiretap Act, which generally prohibits the interception, use, or disclosure of electronic communications (*Id.* §§ 2510 *et seq.*), the Stored Communications Act, which regulates the disclosure of communications held by internet service providers (*Id.* §§ 2701 *et seq.*), and the Pen Registers and Trap and Trace Devices statute, which regulates law enforcement use of devices that record the calls made or received by a phone (*Id.* §§ 3121 *et seq.*). *See* CDT Reply at 8-9.

[1820] Green Class 25 Supp. at 22.

[1821] *Id.*; Bellovin et al. Supp. at 6.

[1822] *See, e.g.*, EFF Class 22 Supp. at 2; *see also id.* at 16 ("The research contemplated by the proposed [C]lass provides a critical public service by identifying potential programming errors that compromise the security and safety of motor vehicles.").

[1823] *See* EFF Class 22 Reply at 14 (stating that a report issued by Senator Markey on auto security concluded that manufacturers' implementation of vehicle software raises consumer security and privacy concerns); *see also* Schneier Class 22 Reply at 2 ("Manufacturers have pointed out that they sometimes work with select, authorized researchers from outside the company to audit their code vulnerabilities. This kind of limited access is not sufficient to provide for secure systems.").

that vehicle recalls based on vehicle software bugs are common,[1824] and cites one instance where "a vehicle manufacturer was found liable for the death of a driver as a result of a software error" after independent researchers identified the error.[1825] Proponents further assert that vehicle software is susceptible to malicious attacks[1826] and cite instances where independent researchers have identified and helped manufacturers resolve security vulnerabilities in vehicle software.[1827]

Although there has thus been some independent research to identify and resolve potentially dangerous vehicle software bugs, proponents maintain that without the prohibition on circumvention, there would be even more.[1828] For instance, Charlie Miller, a vehicle security researcher, testified that he is aware of "other researchers that are very interested in this field" but "will not pursue [it] . . . because they are afraid of the legal problems they would have" under section 1201.[1829] Proponents also claim that "important information [has been] left out of publications about security research such as the identi[t]y of devices and cars being investigated."[1830] Proponents assert that the prohibition's chilling of independent research deprives consumers of the ability to make informed purchasing decisions based on manufacturers' implementation of vehicle

[1824] *See* EFF Class 22 Supp. at 17.

[1825] *Id.* at 18 (citing Michael Dunn, *Toyota's Killer Firmware: Bad Design and Its Consequences*, EDN NETWORK (Oct. 28, 2013), http://www.edn.com/design/automotive/4423428/2/Toyota-s-killer-firmware--Bad-design-and-its-consequences and Michael Barr, *Bookout v. Toyota: 2005 Camry L4 Software Analysis* 5, http://www.sddt.com/files/BARR-SLIDES.pdf (last visited Oct. 7, 2015)).

[1826] *See, e.g.*, EFF Class 22 Reply at 11-12; Green Class 22 Supp. at 1 (citing Stephen Checkoway et al., *Comprehensive Experimental Analysis of Automotive Attack Surfaces*, USENIX Security, 2011, *available at* https://www.usenix.org/legacy/events/sec11/tech/full_papers/Checkoway.pdf and Charlie Miller & Chris Valasek, *A Survey of Remote Automotive Attack Surfaces*, Black Hat, 2014, *available at* http://illmatics.com/remote%20attack%20surfaces.pdf). Though not part of the record in this proceeding, the Register notes that following the public hearings, there were public reports of security researchers' ability to hack into certain Fiat Chrysler manufactured vehicles via the Uconnect internet-connection computer feature, allowing the hacker to remotely control several essential vehicle functions, including steering, brakes, and transmission. *See, e.g.*, Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, WIRED (July 21, 2015), http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway.

[1827] EFF Class 22 Reply at 15 (citing Seth Rosenblatt, *Chinese Hackers Take Command of Tesla Model S*, CNET (July 17, 2014), http://www.cnet.com/news/chinese-hackers-take-command-of-tesla-model-s). In one example, independent researchers identified and helped resolve a vehicle software error that allowed "an attacker to wirelessly unlock a car's doors." EFF Class 22 Supp. at 16 (citing Martyn Williams, *BMW Cars Found Vulnerable in 'Connected Drive' Hack*, PC WORLD (Jan. 30, 2015), http://www.pcworld.com/article/2878437/bmw-cars-found-vulnerable-in-connected-drive-hack.html).

[1828] EFF Class 22 Supp. at 18; *see also id.* at App. B (Statement of Charlie Miller) ("I live in constant fear that the DMCA will be used as a tool by the manufacturers to stop this safety critical research from continuing. I worry that in an effort to stop bad publicity and prevent their customers from getting scared, they will leverage the DMCA against us and the effect will be that everyone's vehicle will be less safe.").

[1829] Tr. at 45:08-13 (May 19, 2015) (Charlesworth, USCO; Miller).

[1830] *Id.* at 9:06-10 (Walsh, EFF).

software.[1831] Proponents thus claim that granting the proposed exemption will "save lives" by enabling independent researchers to identify potentially dangerous vehicle software bugs sooner, and by increasing auto manufacturers' accountability.[1832]

EFF argues that the permanent statutory exemptions under section 1201 are inadequate and "likely to apply only in a narrow subset of scenarios."[1833] EFF contends that section 1201(f)'s reverse engineering exemption may not apply to security research for vehicle software because such research may not meet the requirement of being undertaken for the "sole" purpose of achieving interoperability.[1834] Similarly, proponents maintain section 1201(g)'s encryption research exemption is too narrow to effectively shield independent security researchers from liability under the anticircumvention provisions because security researchers may not be confronted with encryption when examining the security of vehicle ECUs in the first place, and because the multifactor test imposed by that provision imposes unreasonable burdens.[1835] EFF further asserts that the security testing exemption of section 1201(j) is too narrow to apply to independent security researchers who wish to publish their findings in order to advance the state of knowledge in the field, because in that case the information derived from the research would not be used "solely to promote the security of the owner and operator of the vehicle."[1836] In proponents' view, the uncertainty as to the applicability of these several statutory exceptions to various types of security research for vehicle software discourages such research, constituting "a substantial adverse impact that necessitates an exemption."[1837]

[1831] EFF Class 22 Supp. at 16; Schneier Class 22 Reply at 2 ("When researchers are not free to disclose their findings, companies are free to ignore them . . . . If we expect the market to motivate manufacturers to design secure products, there must be consumer-advocate testing and evaluation so that users can make intelligent buying decisions.").

[1832] *See, e.g.*, EFF Class 22 Supp. at 18-20; EFF Class 22 Reply at 15; Schneier Class 22 Reply at 1 ("In fact, obscurity leads to insecurity. When manufacturers are allowed to bar independent researchers from evaluating their products, they can get away with producing shoddy products.").

[1833] *See* 17 U.S.C. § 1201(a)(1)(A); EFF Class 22 Supp. at 19.

[1834] *See* 17 U.S.C. § 1201(f)(1)-(4); EFF Class 22 Supp. at 19 (citing *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 320 (S.D.N.Y 2001)).

[1835] *See* 17 U.S.C. § 1201(g)(2); EFF Class 22 Supp. at 20-21; *see also* EFF Class 22 Supp. at 21 ("[Independent security researchers] may not to provide the copyright owner with notice of their findings [as required by section 1201(g)(3)(C)], depending on whether they think the copyright owner will act receptively or negatively."); Schneier Class 22 Reply at 2.

[1836] *See* 17 U.S.C. § 1201(j)(3)(A) ("In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include (A) whether the information derived from the security testing was used solely to promote the security of the owner or operator of such computer, computer system or computer network . . ."); EFF Class 22 Supp. at 22.

[1837] EFF Class 22 Supp. at 22; *see also* Schneier Class 22 Reply at 2 ("I know many security researchers who have refrained from conducting important security research because they fear the DMCA. All future research is harmed by this chilling effect.").

iii. Proposed Class 27A: Medical Device Software – Security and Safety Research

Regarding Class 27A, MDRC contends that independent security research is critical to the safety and security of millions of Americans who rely on the software used in implanted medical devices.[1838] According to MDRC, "[c]omputerized medical devices can fail in many ways, including through programming errors, incorrect calibration, and exposure to malicious intrusions, as well as physical or medical errors."[1839] It observes that hundreds of deaths have occurred as a result of software-related errors in medical devices,[1840] and a significant percentage of medical device recalls involve software errors.[1841] In its view, independent research on medical device software "effectively addresses these problems" by "analyzing the design flaws and vulnerabilities of medical devices."[1842] MDRC also contends device manufacturers' current research efforts do not sufficiently address the safety and security threats posed by medical device software.[1843]

MDRC notes that most earlier research on medical device software has not implicated anticircumvention law at all because medical devices have not typically employed TPMs.[1844] But manufacturers are increasingly using TPMs to protect medical device software for various reasons.[1845] In particular, proponents note that recent guidance issued by the Food and Drug Administration ("FDA") recommends that manufacturers impose TPMs to protect device security and patient privacy, such as by limiting access to data through passwords, code authentication, and encryption of wireless communications.[1846] Proponents assert that those recommendations are likely to

---

[1838] MDRC Supp. at 2, 18.

[1839] *Id.* at 2.

[1840] *Id.* at 2, 18 (citing Homa Alemzadeh et al., *Analysis of Safety-Critical Computer Failures in Medical Devices*, 11 IEEE SECURITY & PRIVACY 14, 22 (2013) ("Alemzadeh et al.").

[1841] *Id.* at 18 (citing FDR CTR. FOR DEVICES AND RADIOLOGICAL HEALTH: 510(K) WORKING GROUP, PRELIMINARY REPORT AND RECOMMENDATIONS (2010), *available at* http://www.fda.gov/downloads/AboutFDA/CentersOffices/CDRH/CDRHReports/UCM220784.pdf).

[1842] *See id.* at 3, App. B.

[1843] *Id.* at 20 ("There is great incentive for the medical device manufacturers to deter independent discovery of vulnerabilities, because there is such a profound economic disincentive for manufacturers to have these vulnerabilities come to light.").

[1844] *See id.* at 3, 19-20; MDRC Reply at 2-3.

[1845] *See, e.g.*, MDRC Supp. at 2 (citing Alemzadeh et al. at 14, 22) (attributing manufacturers' implementation of TPMs in medical device software to increased use in recent years); *id.* (citing David Talbot, *Computer Viruses Are "Rampant" on Medical Devices in Hospitals*, MIT TECH REV. (Oct. 17, 2012), http://www.technologyreview.com/news/429616/computerviruses-are-rampant-on-medical-devices-in-hospitals) (stating manufacturers' implementation of TPMs in medical device software is due to concerns raised by scholars that devices are vulnerable to malicious hacking).

[1846] *Id.* at 7, 9 (citing FDA, CONTENT OF PREMARKET SUBMISSION FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 4 (Oct. 2, 2014), *available at* http://www.fda.gov/downloads/medicaldevices/deviceregylationandguidance/guidance documents/ucm356190.pdf ("FDA PREMARKET SUBMISSION GUIDANCE") and FDA, RADIO FREQUENCY

be adopted by the medical device industry and lead to an increase in the application of TPMs; they explain that "[g]uidance documents like these, while not legally binding, are the usual means by which the FDA indicates its preferences when examining devices, and entities regulated by the FDA routinely treat these guidelines as rules in order to assure expediency in FDA approvals."[1847] MDRC thus predicts that legitimate independent research will be chilled as more and more medical devices become subject to section 1201(a)(1).[1848]

In supporting the requested exemption, Public Knowledge opines that the permanent statutory exemptions to section 1201's anticircumvention provision are insufficient because "[t]he uncertainty around the various specifics of the statutory exemptions can restrict the activities of researchers and patients in a number of ways that stymie useful work."[1849]

d. Argument Under Statutory Factors

i. Proposed Class 25: Software – Security Research

Proponents maintain that the statutory factors set forth in 1201(a)(1) support a broad exemption for software security research.

On the availability for use of copyrighted works, Class 25 proponents assert that as a result of the DMCA prohibition, "security researchers are creating fewer publications relating to information security research."[1850] Green argues as well that with the requested exemption, researchers would be able to render software and the devices it controls "more useful and more valuable."[1851] Bellovin et al. contend that with an exemption in place that allowed public disclosure, "[m]ore copyrighted works would be created, and the work would be of even higher caliber," such as "new, stronger access controls" created in response to the discovery of vulnerabilities in previous access controls, more products that "compete on the basis of software security," and consumer safety reports and articles about vulnerabilities.[1852]

Regarding the second factor, Class 25 proponents assert that an exemption would increase the availability for use of works for nonprofit educational purposes because section 1201(a)(1)'s prohibition, and the accompanying risk of liability, "forces

---

WIRELESS TECHNOLOGY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 10-11 (Aug. 14, 2013)).

[1847] *Id.* at 9.

[1848] *See id.* at 20; *see also, e.g.*, Schneier Class 27 Reply at 2; Green Class 27 Supp. at 1; Public Knowledge Class 27 Reply at 5.

[1849] Public Knowledge Class 27 Supp. at 7.

[1850] *See, e.g.*, Bellovin et al. Supp. at 8.

[1851] Green Class 25 Supp. at 22-23.

[1852] Bellovin et al. Supp. at 8; Bellovin et al. Reply at 5-7.

researchers to limit student involvement and can push risk-averse universities from such research," as well as interfere with "research approval and funding."[1853]

On the third factor, Class 25 proponents assert that the prohibition has had a negative impact on criticism, comment, news reporting, teaching, scholarship and research by chilling security researchers from engaging in good-faith security research, "hindering the security of critical information infrastructure,"[1854] "damaging classroom teaching of future generations of students about the mechanics of computer security,"[1855] and allowing companies to use copyright law "to limit criticism, comment or news reporting about . . . insecurities."[1856] Bellovin et al. argue that an exemption would, by contrast, stimulate the above activities, such as by allowing "for secondary analysis and critique by the press to arise regarding security of consumer products."[1857]

On the fourth factor, Class 25 proponents contend that an exemption will not harm the market for or value of copyrighted works,[1858] but instead would have a "positive net effect on the market for software and devices," as any negative impact on the market would "result only from the exposure of inherent shortcomings in the works themselves."[1859] Furthermore, Green asserts that "coordinated disclosure guidelines" for research findings would help "reduce the risk of market impacts by allowing companies time to address vulnerabilities before they are made public," creating a greater incentive to secure and repair software, thus increasing its quality and value, and the safety and security of consumers.[1860]

Proponents also raise, under the fifth statutory factor, a number of other considerations that they believe weigh in favor of an exemption. Proponents argue that if an exemption is granted, security researchers in academic, government and corporate settings will be better poised to address consumer safety issues by exposing

---

[1853] Green Class 25 Supp. at 23; *see also* Bellovin et al. Supp. at 8 (contending that "information security education efforts are actively hampered [by the prohibition] on all levels of the educational system"); Tr. at 160:18-22 (May 26, 2015) (Bellovin) ("I cannot do grant-funded research that, with a contract, gives somebody else the right, precisely to preserve academic freedom and also to protect me and my students under the export laws."); Tr. at 75:05-76:12 (May 26, 2015) (Blaze).

[1854] Green Class 25 Supp. at 23; *see also* Bellovin et al. Supp. at 8; Stanislav Supp. at 1; Perry Reply at 1.

[1855] Stolfo Supp. at 1.

[1856] CDT Reply at 9-10; *see also* Tr. at 38:01-07 (May 26, 2015) (Sayler on behalf of Green); Tr. at 204:21-205:04 (May 26, 2015) (Bellovin).

[1857] Bellovin et al. Supp. at 8; Bellovin et al. Reply at 11.

[1858] Brown et al. Supp. at 1 (arguing that "no negative repercussions will arise with respect to the safety or security of software from granting this exemption"); *see also* Internet Association Supp. at 1; Rapid7 Supp. at 1; Stolfo Supp. at 1; VVF Supp. at 1.

[1859] Green Class 25 Supp. at 24; *see also* Bellovin et al. Reply at 11 (contending that "[t]he market for and value of copyrighted works that researchers have found to be well-coded will significantly increase if this exemption is granted"); Tr. at 45:06-15 (May 26, 2015) (Stanislav, Rapid7).

[1860] Green Class 25 Supp. at 24.

vulnerabilities in the face of evolving cybersecurity risks and "defend[ing] national and international security interests, critical infrastructure, and the economies of both the United States and its trusted allies" as well as "corporate intellectual property assets . . . [and] the data of the consumers."[1861] Bellovin et al. contend that, without an exemption, "the market fails to incorporate accurate information regarding quality of security in products" and subsequently "undervalues companies that invest in security and overvalues those that do not."[1862] In addition, OTI notes that an exemption is necessary because the Federal Trade Commission and many state governments require vendors to keep personal information secure, and these governmental entities sometimes rely on the work of independent security researchers to identify noncompliant vendors.[1863]

Responding to a point made by a number of opponents, described in greater detail below, proponents argue that the section 1201 rulemaking proceeding is not the appropriate forum to address non-copyright issues relating to security research, such as concerns that security researchers could violate other laws or regulations.[1864] Bellovin et al. assert that if an exemption were granted, "copyright holders [would still] retain all non-DMCA recourse options against security researchers and all regulatory obligations under every other legal regime," such as recourse under the CFAA and regulations promulgated by other agencies such as FDA.[1865] Accordingly, proponents argue that any exemption should not incorporate laws unrelated to copyright, such as the CFAA, the Clean Air Act ("CAA"), trade secret law, or other laws and regulations, as other administrative and law enforcement agencies are better equipped to address and enforce those laws and regulations and incorporating such laws into the proposed exemption could create more uncertainty.[1866]

A significant issue raised with respect to all of the proposed research classes is the extent to which any exemption should incorporate a requirement that flaws uncovered by security researchers be disclosed to the software developer and/or product manufacturer before being communicated to the public at large. As discussed in greater depth below,

---

[1861] Brown et al. Supp. at 1; Internet Association Supp. at 1; *see also* Bellovin et al. Supp. at 9 (contending that an exemption "would enable security research into products particularly designed for children," such as insulin pumps for child diabetics); Andersen et al. Supp. at 1; Green Class 25 Supp. at 25; Rapid7 Supp. at 1; Stolfo Supp. at 1; VVF Supp. at 1; Tr. at 38:25-39:04 (May 26, 2015) (Sayler on behalf of Green).

[1862] Bellovin et al. Supp. at 8.

[1863] Tr. at 98:18-100:09 (May 26, 2015) (Moy, OTI).

[1864] Green Class 25 Reply at 2, 5 (contending that "[t]o whatever extent concerns over automotive and medical software are legitimate, the triennial review is not the appropriate forum in which to address the contours of automotive and medical policy"); OTI Class 25 Reply at 6 (noting that "the fact that this proceeding has veered into such areas that Congress never intended is as good a proof as any that the DMCA's anti-circumvention provisions are having a worrisomely overbroad impact far beyond the scope of copyright law"); Tr. at 145:19-146:05 (May 26, 2015) (Reid on behalf of Green).

[1865] Bellovin et al. Reply at 8-9.

[1866] CDT Post-Hearing Resp. at 4-5; *see also* Green Post-Hearing Resp. at 5; Matwyshyn et al. Post-Hearing Resp. at 6.

opponents argue that if the Register recommends an exemption for software security research, she should also recommend an express disclosure requirement, so that the software developer or product manufacturer has sufficient time to correct any flaw before its existence becomes more widely disseminated and thus more susceptible to exploitation by malicious actors.

Some proponents argue that there should be no disclosure requirement attached to any proposed exemption, finding it to be unnecessary in light of the fact that good-faith security researchers already follow various best-practice disclosure guidelines and standards.[1867] Proponents assert that if researchers are not allowed the discretion to disclose their findings as they see fit, companies may feel free to ignore the existence of the identified flaws.[1868] Proponents also argue that the Copyright Office is not the appropriate body, nor the section 1201 rulemaking the appropriate forum, to address the complex and controversial issue of reasonable vulnerability disclosure practices.[1869] These proponents further argue that security research and disclosure of such research is protected by the First Amendment.[1870] They thus contend that creating a requirement to first disclose vulnerabilities to copyright owners and/or product manufacturers would raise significant concerns under the First Amendment as it "would constitute a restriction on protected speech."[1871]

Other proponents argue that a disclosure standard may be appropriate, but that any such standard should be flexible. In their view, disclosure before publication or other public disclosure must be dealt with on a "case-by-case basis" since, in some cases, "it may be more prudent to warn the public immediately" than to wait for a manufacturer response.[1872]

[1867] CDT Post-Hearing Resp. at 2-3 (citing "published guidelines [that] offer best practices for disclosing security vulnerabilities in a variety of situations," including ones produced by the Internet Engineering Task Force and the CERT Division of the Software Engineering Institute).

[1868] Schneier Class 25 Reply at 1.

[1869] *See, e.g.*, Green Class 25 Reply at 12 (arguing that "[i]t is beyond the scope of this proceeding to consider, much less address, the serious ramifications of disclosure policy"); CDT Reply at 10 (asserting that neither the Office nor rightsholders should "dictate when research should be conducted or disclosed").

[1870] Green Class 25 Supp. at 25; *see also* Green Class 25 Reply at 15; CDT Post-Hearing Resp. at 3; Green Post-Hearing Resp. at 2-3; Matwyshyn et al. Post-Hearing Resp. at 3-4; Tr. at 85:08-22 (May 26, 2015) (Reid on behalf of Green).

[1871] Green Post-Hearing Resp. at 2. In particular, Green argues that "[a] regulation preventing researchers from publicly disclosing a vulnerability until a certain period of time after they disclose the same vulnerability" to the vendor "would constitute a restriction on protected speech." *Id.* (citing *Universal City Studios v. Corley*, 273 F.3d 429, 447 (2d Cir. 2001)). Green also argues that any restriction in the content of what researchers publish would "aim directly at the content of protected speech," and so "must be the least restrictive means of achieving a compelling interest to pass First Amendment muster." *Id.* (citing *Sable Commc'ns of Cal., Inc. v. FCC*, 492 U.S. 115, 126 (1989)).

[1872] Tr. at 80:04-20 (May 26, 2015) (Blaze); *see also id.* at 80:22-82:06 (Green); CDT Post-Hearing Resp. at 1-3; Green Post-Hearing Resp. at 3-5 (arguing that any disclosure requirement should adopt "a flexible approach that ensures that any uncertainty about the propriety of any public disclosure errs in favor of

A number of proponents propose that the Librarian look to the international vulnerability disclosure standards promulgated by the International Organization for Standardization ("ISO") for guidance because they "provide[] a floor of corporate conduct" and "embody security practices already implemented by responsible corporate entities . . . , creat[ing] a logical balance between information security and intellectual property protection in the private sector."[1873] In response to opponents' objection that the ISO standards are proprietary and not publicly available, Bellovin et al. offered "reasonable vulnerability management practices" that they claim mirror the ISO standards and would facilitate appropriate disclosure.[1874]

For its part, CDT urges the Office to refrain from using section 1201(j) as a model for any disclosure requirements in the proposed exemption because, as noted above, proponents contend that section 1201(j) is ambiguous and may practically foreclose certain security research.[1875]

Of particular concern is that whether an act of circumvention is considered permissible under section 1201(j) depends upon the weighing of a number of factors rather than a bright-line rule. To assess whether circumvention was legitimate, section 1201(j) calls for consideration of "whether the information derived from the security testing was used solely to promote the security of the owner or operator of such computer, computer system or computer network, or shared directly with the developer of such computer, computer system, or computer network" and "whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security." [1876]

Finally, proponents responded to a concern raised by BSA | The Software Alliance ("BSA")[1877] and the Office regarding the appropriateness of security research being performed on a "live" or "active" system, such as medical devices in use by patients or vehicles in use on public roads.[1878] The issue was pointedly addressed in the hearings, in part due to news reports suggesting that a security researcher had conducted unauthorized research on an in-flight commercial airliner.[1879] In response to the Office's questioning, there appeared to be universal agreement among proponents that testing of "live systems"

---

allowing the researcher to proceed"); Matwyshyn et al. Post-Hearing Resp. at 2-3 (referencing vulnerability management practices related to disclosure); Bellovin et al. Reply at 1-2 (same).

[1873] Brown et al. Supp. at 1 (citing ISO 29147 and ISO 30111); *see also* Internet Association Supp. at 1; Bellovin et al. Supp. at 10; Stolfo Supp. at 1.

[1874] Bellovin et al. Reply at 1-2; *see also* Tr. at 57:24-61:20 (Matwyshyn).

[1875] CDT Post-Hearing Resp. at 3-4.

[1876] 17 U.S.C. § 1201(j)(3).

[1877] BSA Class 25 Opp'n at 2, 5.

[1878] Tr. at 137:19-138:25 (May 26, 2015) (Charlesworth, USCO).

[1879] *Id.*

is inappropriate and is not an activity they seek to have covered by the requested exemption.[1880] As Professor Green stressed in a post-hearing submission, "researchers performing their duties in good faith never conduct research on live systems actively protecting critical infrastructure, medical devices while implanted in patients, or vehicles while in use for nonresearch purposes."[1881]

ii. Proposed Class 22: Vehicle Software – Security and Safety Research

Regarding the first statutory consideration, EFF asserts that the proposed exemption in Class 22 will increase, rather than limit, the availability of copyrighted works for public use.[1882] In EFF's view, copyrighted vehicle software is not fully available for "use" in the absence of an exemption.[1883] EFF maintains that the proposed exemption would increase the public's ability to use such works by allowing individuals to access the software for security research purposes.[1884] EFF further asserts that additional copyrighted works, such as software patches and publications, would be made available based upon the research facilitated by the proposed exemption.[1885]

EFF asserts that the second factor weighs in favor of the proposed exemption because security research for vehicle software is fundamentally educational in nature.[1886] In EFF's view, absent an exemption, there is virtually no way to "engage in nonprofit archival, preservation, and educational uses of vehicle software subject to technological restrictions."[1887] Accordingly, EFF maintains that the proposed exemption will broaden the public's ability to engage in those uses of copyrighted works.[1888]

With respect to the third factor, EFF asserts that "[r]esearch is obviously at the core of the proposed exemption, and the adverse effects of prohibition demonstrate that

---

[1880] *See, e.g.*, *id.* at 150:16-29 (Blaze) ("[L]et me add my voice to the chorus that condemns tampering with live safety, critical systems. I think nobody—nobody advocates that here."); *id.* at 139:03-08, 141:15-20, 23-25 (Green); *id.* at 144:02-06 (Reid on behalf of Green).

[1881] Green Post-Hearing Resp. at 1 n.3.

[1882] *See, e.g.*, EFF Class 22 Supp. at 22; EFF Class 22 Reply at 17.

[1883] EFF Class 22 Reply at 17-18.

[1884] EFF Class 22 Supp. at 22-23; EFF Class 22 Reply at 17-18.

[1885] *See* EFF Class 22 Supp. at 23 ("Craig Smith, author of the *2014 Car Hacker's Handbook*, reported that the *Handbook* was downloaded 300,000 times in the first two weeks it was available. Software patches also depend on access, including patches to fix serious vulnerabilities. Numerous tools designed to analyze and manipulate firmware also depend on the ability to access software and reverse engineer it.").

[1886] *See, e.g.*, *id.*; EFF Class 22 Reply at 18.

[1887] EFF Class 22 Reply at 18.

[1888] *See, e.g.*, EFF Class 22 Supp. at 23 ("In addition, it will be possible to archive and preserve firmware on general-purpose storage media, without expensive and unreliable storage of ECU hardware removed from a vehicle."); EFF Class 22 Reply at 18 (stating the proposed exemption would facilitate conducting educational security research at universities).

the factor weighs in favor of an exemption."[1889] More specifically, proponents contend that the threat of liability hampers legitimate security research efforts for vehicle software, and also prevents reporting, criticism and commentary on security vulnerabilities in vehicle software.[1890]

As for the fourth factor, EFF asserts that the market for vehicle software will not suffer any harm cognizable under copyright law, because "[c]opyright law only recognizes economic harm where a proposed use usurps the demand for the original."[1891] EFF maintains that "[n]either copyright law nor good public policy protects a manufacturer's interests in *not fixing* product defects" once they are revealed due to an increase in vehicle software security research.[1892] EFF also submits that the proposed exemption will actually increase the value of copyrighted works, because greater involvement in vehicle software security research will increase the software's value by improving overall vehicle safety and security.[1893]

With respect to the fifth factor, addressing such other factors as the Librarian considers appropriate, EFF asserts that "[t]he Librarian should grant an exemption that does not depend on a vehicle owner's status as an owner or licensee of [vehicle computer programs]."[1894] EFF also contends that "the exemption should permit circumvention done with the permission of the owner of a vehicle by a third party."[1895] According to EFF, such an exemption would not violate the anti-trafficking provisions of section 1201(a)(2) because security research for vehicle software "does not fall under any of the three categories of forbidden conduct identified in 1201(a)(2)(A) through (C)," namely, offering technologies or services that are "primarily designed or produced for the purpose of circumventing" a TPM, that have "only limited commercially significant purpose or use other than to circumvent" a TPM, or are "marketed . . . for use in circumventing" TPMs.[1896] In response to comments made by opponents, EFF also asserts existing tort and criminal laws are more aptly suited than the anticircumvention provisions to safeguard the public against malicious attacks on vehicle software.[1897] EFF also contends that opponents' concerns that vehicle security research will cause vehicles to be out of compliance with fuel economy, emissions, and safety standards are overstated or

[1889] EFF Class 22 Reply at 19.

[1890] *See, e.g.*, Schneier Class 22 Reply ("I know of many security researchers who have refrained from conducting important security research because they fear the DMCA. I know of even more security research where the results are not being published because the researchers fear the DMCA."); EFF Class 22 Supp. at 23; EFF Class 22 Reply at 19; Green Class 22 Supp. at 1.

[1891] EFF Class 22 Reply at 19.

[1892] *Id.* (emphasis in original).

[1893] *Id.* at 20.

[1894] EFF Class 22 Supp. at 24.

[1895] *Id.*

[1896] *See* 17 U.S.C. § 1201(a)(2)(A)-(C); EFF Class 22 Supp. at 24-25.

[1897] EFF Class 22 Reply at 19.

mischaracterize the nature of such research.[1898] EFF adds that "opponents' claims regarding the risk posed by modification of vehicle software and the difficulty of detecting modified software are overblown at the very least," as "tamper-evident flags and software checksums are simple measures to detect software changes."[1899]

iii. Proposed Class 27A: Medical Device Software – Security and Safety Research

Concerning the first statutory factor, MDRC asserts that the proposed exemption in Class 27A would benefit rather than harm the availability for use of copyrighted works.[1900] According to MDRC, given that patients use medical device software regardless of whether TPMs are in place, the proposed exemption would only increase the public's ability to use copyrighted works by allowing independent researchers to access medical device software for research purposes.[1901] MDRC also suggests that new copyrighted works will be published as a result of information made available under the proposed exemption.[1902]

MDRC maintains that the second factor weighs in favor of the proposed exemption, because independent research of medical device software can be undertaken for educational purposes.[1903] In support of this claim, MDRC offers that "there are now numerous conferences and other gatherings between independent researchers and manufacturers, including those convened by the FDA and universities."[1904] In MDRC's view, the use of medical device software for nonprofit educational purposes "is entirely unavailable for a device employing a TPM unless this exemption is granted."[1905]

With respect to the third factor, MDRC asserts that "the improvement of scholarship and research around the safety of medical devices, both in general and as applied to particular patients, is the essence of the exemption requested here."[1906] Accordingly, MDRC maintains that the proposed exemption "will lead to advances in the medical research field."[1907] It further suggests that the proposed exemption should

---

[1898] *Id.* ("At the outset, it is worth noting that the vast majority of the activities contemplated within the proposed class do not involve the operation of modified vehicles on public roadways . . . .").

[1899] *Id.* at 21.

[1900] MDRC Supp. at 23.

[1901] *Id.* at 23-24.

[1902] *See, e.g.*, *id.* at 11-13, 20 (stating the proposed exemption will facilitate the publication of articles based on findings of medical device software researchers).

[1903] *See, e.g.*, MDRC Reply at 16 (stating independent research of medical device software occurs at state university-affiliated research centers).

[1904] *Id.* at 6.

[1905] MDRC Supp. at 24.

[1906] *Id.*

[1907] *Id.*

"allow for the owners and operators of medical devices to solicit the help of others in conducting this research."[1908] According to proponents, the current threat of liability resulting from section 1201's prohibition on circumvention hinders legitimate research efforts and suppresses researchers' efforts to publicly disclose their findings through criticism, commentary, scholarship and reporting.[1909]

Regarding the fourth factor, MDRC cites to the Register's conclusion in the 2006 rulemaking that "research into and correction of security flaws in access controls ultimately will have a positive impact on the market for or value of copyrighted works."[1910] MDRC argues by analogy that the independent research on medical device software that would be facilitated by the proposed exemption "can only improve the market for these devices."[1911] MDRC further asserts that as this research continues, "the public will become more confident in the safety of these devices, and thus increase demand in the market."[1912] Moreover, the market value for the work will not be harmed in a copyright law sense because "[c]onducting this research does not usurp the demand for the original devices, as no copy that is made in the process of developing this research could ever replace the need for a medical device."[1913]

Proponents do not expressly discuss the fifth factor, allowing consideration of such other factors as the Librarian deems appropriate, although they maintain that failing to grant the proposed exemption may contravene the President's cybersecurity policy as well as FDA's policy for medical devices, which seeks to increase the timeliness and quality of information regarding cyber threats.[1914]

Proponents also maintain that the safety and security concerns raised by opponents are overstated, and that the evidence suggests that software programming errors—rather than attacks by wrongdoers—pose the greater threat to medical device users. They note that "the concept that insecure systems can overcome their shortcomings by keeping security-related details secret" has been widely rejected by scholars and government agencies.[1915]

[1908] *Id.* at 21.

[1909] *See, e.g.*, *id.* at 20 ("Given the presence of TPMs on some of these devices, [independent researcher Jerome Radcliffe] sought counsel to analyze whether his research would present a risk under the DMCA. Ultimately, he was forced to limit his inquiry to the portions of the devices that were not protected by the TPM . . . . In another context, legal ambiguity and the lack of clear exemptions lead a major technology publisher to cancel release of a significant computer science book on hardware reverse engineering."); Schneier Class 27 Reply at 2; Green Class 27 Supp. at 1.

[1910] MDRC Supp. at 25 (citing 2006 Recommendation at 64).

[1911] *Id.*

[1912] *Id.*

[1913] *Id.*

[1914] *See id.* at 18; MDRC Reply at 7, 18-20

[1915] *See* MDRC Supp. 22-23; Schneier Class 27 Supp. at 1.

Finally, proponents make clear that their request is not intended to extend to security research on individual devices that are used, or intended to be used, on or for patients during or after the security research.[1916]

2. Opposition

The Office received comments in opposition to the general software security research exemption in Class 25 from AdvaMed, Auto Alliance, BSA, General Motors ("GM"), Intellectual Property Owners Association ("IPO"), LifeScience Alley, Medical Device Innovation Safety and Security Consortium ("MDISS"), and Software Information Industry Association ("SIIA").[1917]

The vehicle software security research exemption in Class 22 was opposed by Association of Global Automakers ("Global Automakers"), Auto Alliance, GM, John Deere, and Motor & Equipment Manufacturers Association ("MEMA").[1918]

The medical device software security exemption in Class 27A was opposed by AdvaMed, IPO, Jay Schulman, LifeScience Alley, and National Association of Manufacturers ("NAM").[1919]

As indicated above, the proposed general software security research exemption represented by Class 25 is broad enough to swallow the more specific exemptions for vehicle software security research in Class 22 and medical device software security research in Class 27A. Much of the substantive opposition to the general software security research exemption in Class 25 came from parties whose core interests pertain to vehicles and medical devices. As such, some of the opposition analysis in Class 25 is repeated in Classes 22 and 27A. Nonetheless, to maintain consistency with the approach taken with respect to the proponents' arguments, the Register separately addresses the opposition arguments made in each class.

[1916] *See* Tr. at 34:14-24 (May 29, 2015) (Sellars, MDRC; Charlesworth, USCO).

[1917] AdvaMed Class 25 Opp'n; Auto Alliance Class 25 Opp'n; BSA Class 25 Opp'n; GM Class 25 Opp'n; IPO Class 25 Opp'n; LifeScience Alley 25 Opp'n; MDISS Opp'n; SIIA Class 25 Opp'n.

[1918] Auto Alliance Class 22 Opp'n; Global Automakers Class 22 Opp'n; John Deere Class 22 Opp'n; MEMA Class 22 Reply. The Register notes that MEMA filed its comments in the reply phase of the written comment period, which had been designated as allowing proponents and neutral commenters to respond to points made by the opposition. The Register will exercise her discretion to consider MEMA's comments in reply, while at the same time being mindful that proponents did not have an opportunity to file written comments in response to MEMA.

[1919] AdvaMed Class 27 Opp'n; IPO Class 27 Opp'n; Schulman Opp'n; LifeScience Alley Class 27 Opp'n; NAM Opp'n.

a. Asserted Noninfringing Uses

i. Fair Use

1) Proposed Class 25: Software – Security Research

Opponents argue that Class 25 proponents have failed to establish that the uses sought under the general proposed exemption for software security research are noninfringing.[1920] While BSA did not offer an analysis under the fair use factors, it contends that "proponents seek to engage in such a wide variety of activities that it is impossible to assess whether all of these activities qualify as non-infringing."[1921] While AdvaMed likewise declines to analyze the claim that the proposed uses under Class 25 would be noninfringing, it suggests that they would not be, asserting that "[a]llowing circumvention activities [that] would lead to exposure of medical device source code" would exceed any license terms attached to the sale of the devices, and would result in the loss of "intellectual property."[1922] AdvaMed also urges that "allowing access to and reverse engineering of source code would likely increase the number of knock-off products, because once the source code is obtained it could easily be transmitted to anyone in the world or posted on the Internet."[1923]

Opponent GM does address the fair use factors, arguing that proponents' fair use analysis is flawed.[1924] For the first factor, GM contends that the purpose and character of the use should disfavor a finding of fair use, because "the dissemination of highly sensitive information about how a car's ECUs or TPMs operate increases the potential risk that even individuals with benign intent might access and modify their vehicle software in such a manner that increases, rather than minimizes security and safety challenges."[1925] GM asserts that the second factor also weighs against fair use because vehicle software "is a highly creative work designed by specialized engineers" and because the "mere existence of certain functional elements does not obviate the need to protect the expressive aspects also encompassed in the work."[1926] GM contends that the third factor weighs against a finding of fair use because proponents "seek to copy an entire work."[1927] GM argues that the fourth factor also weighs against a finding of fair use because the uses sought by proponents would "directly and negatively" affect the value of the copyrighted works by allowing "individuals to access, analyze, modify and

[1920] *See, e.g.*, GM Class 25 Opp'n at 9.

[1921] BSA Class 25 Opp'n at 4. However, BSA explains that it would be comfortable with an exemption narrowly tailored to "specific types of access controls that [are] creating security vulnerabilities." Tr. at 136:02-23 (May 26, 2015) (Troncoso, BSA; Charlesworth, USCO).

[1922] AdvaMed Class 25 Opp'n at 3-4.

[1923] *Id.* at 6.

[1924] GM Class 25 Opp'n at 9-12.

[1925] *Id.* at 10.

[1926] *Id.* at 10-11.

[1927] *Id.* at 11.

then publish code for vehicle software," which "risks increasing, not diminishing vehicle safety and security challenges."[1928]

2) Proposed Class 22: Vehicle Software – Security and Safety Research

Class 22 opponents similarly challenge the view that vehicle security and safety research activities constitute noninfringing fair use.[1929] Under the first fair use factor, opponents argue that consideration of the purpose and character of the use weighs against a fair use finding.[1930] Several opponents find fault in particular with proponents' assertion that security research serves the public interest and contend that allowing disclosure of sensitive information would instead adversely affect safety, security and the regulatory landscape.[1931] John Deere additionally asserts that the exemption would enable and encourage noncompliance with environmental regulations, and that such a use is of a purpose and character that should be disfavored under section 107.[1932]

In opponents' view, the second fair use factor, the nature of the copyrighted work, also favors a finding that the proposed uses do not qualify as fair use.[1933] John Deere recognizes that the computer programs on ECUs are functional in nature, but notes that they also contain certain creative elements.[1934] John Deere further contends that the TPMs for vehicle software are not only used to protect against infringement of creative software programs, but also "highly-expressive" works such as music, television content, and movies that are played via in-vehicle entertainment systems.[1935] GM also asserts that the computer programs at issue are highly creative and expressive, noting the time and resources devoted to their development.[1936] It thus urges that while elements of such computer programs are functional in nature, that does not obviate the need to protect the programs' creative expression.[1937]

[1928] *Id.* at 11-12.

[1929] *See, e.g.*, Global Automakers Class 22 Opp'n at 4-6; GM Class 22 Opp'n at 11-13; John Deere Class 22 Opp'n at 5-8.

[1930] *See, e.g.*, Global Automakers Class 22 Opp'n at 4-5; GM Class 22 Opp'n at 11; John Deere Class 22 Opp'n at 6.

[1931] GM Class 22 Opp'n at 11; *see also* Global Automakers Class 22 Opp'n at 4-5 (noting that "the proposed exemption does not even clarify whether the proposed uses seek to *improve* the security and safety of automobiles, meaning even those that intentionally seek to *impede* safety and security would qualify") (emphasis in original).

[1932] John Deere Class 22 Opp'n at 6 .

[1933] *See, e.g., id.* at 7; GM Class 22 Opp'n at 11-12; Global Automakers Class 22 Opp'n at 5.

[1934] John Deere Class 22 Opp'n at 7.

[1935] *Id.*

[1936] GM Class 22 Opp'n at 12; *see also* Global Automakers Class 22 Opp'n at 5; Tr. at 61:01-09 (May 19, 2015) (Lightsey, GM).

[1937] GM Class 22 Opp'n at 12; *see also* Global Automakers Class 22 Opp'n at 5.

With respect to the third fair use factor, addressing the amount and substantiality of the uses, opponents uniformly maintain that the proposed uses require copying of the bulk, if not the entirety, of the computer programs.[1938] Additionally, they observe that the essential part of the work will remain in the modified copy.[1939] Therefore, they conclude that the third factor strongly indicates that the proposed uses are not fair.[1940]

Turning to the fourth factor, regarding the impact on the market for or value of the work, opponents assert that vehicle values may be adversely affected by an exemption.[1941] Opponents argue that if the exemption is granted, vehicles are likely to become out of compliance with regulatory standards in areas such as fuel economy, emissions control, and safety, which they assert could negatively impact the ability to resell the car, or a subsequent purchaser's ability to meet state vehicle registration requirements.[1942] John Deere also asserts that the activity covered under the exemption could erode the public's trust in the safety and security of vehicles, thereby diminishing demand for new vehicles.[1943] Global Automakers further contends that an exemption would damage and disrupt safety and security research programs in which automobile manufacturers currently engage with vetted third parties, such as universities, hospitals and other research institutions.[1944]

Auto Alliance takes a different tack in criticizing proponents' fair use argument, asserting that it "fails because it is based on a false premise about prior exemptions" granted by the Librarian.[1945] Auto Alliance argues that the 2006 and 2010 exemptions on which EFF relies to assert that the activities of security researchers constitute fair use are distinguishable from the proposed exemption because they "were limited to testing, investigating and correcting security flaws that were caused by access controls," whereas the proposed exemption has no such limitation.[1946] While Auto Alliance concedes that the Register concluded in previous rulemakings that there was uncertainty surrounding the applicability of section 1201(j) to the uses proposed in 2006 and 2010, Auto Alliance nonetheless contends that any questions posed by the Register in those rulemakings about the scope of section 1201(j) "are completely irrelevant" to the exemption proposed here because it does not involve vulnerabilities caused by access controls. Thus, per Auto

---

[1938] *See, e.g.*, John Deere Class 22 Opp'n at 8; GM Class 22 Opp'n at 12; Global Automakers Class 22 Opp'n at 5.

[1939] *See, e.g., id.*

[1940] *See, e.g., id.*

[1941] *See, e.g.*, John Deere Class 22 Opp'n at 8; GM Class 22 Opp'n at 13; Global Automakers Class 22 Opp'n at 5-6.

[1942] *See, e.g.*, John Deere Class 22 Opp'n at 8; GM Class 22 Opp'n at 13.

[1943] John Deere Class 22 Opp'n at 8.

[1944] Global Automakers Class 22 Opp'n at 5-6.

[1945] Auto Alliance Class 22 Opp'n at 6.

[1946] *Id.* at 6-8.

Alliance, a "*de novo* consideration" of security research and the applicability of section 1201(j) is required in the current proceeding.[1947]

3) Proposed Class 27A: Medical Device Software – Security and Safety Research

Class 27A opponents present only limited argument to counter proponents' claim that security research conducted on medical device software constitutes a fair use. AdvaMed maintains that independent researchers' use of medical device computer programs is for a commercial purpose, and so weighs against a finding of fair use.[1948] Opponents do not offer analysis of the second fair use factor. AdvaMed contends that the third fair use factor weighs against a finding of fair use because proponents seek to use an excessive amount of the work in the course of conducting their research.[1949] In relation to the fourth fair use factor, opponents do not expressly present evidence demonstrating that independent research on medical device software would cause market harm by supplanting demand for the original work, but they do maintain such research would negatively impact the market for medical device software in other ways, such as by "caus[ing] patients to decide against an appropriate [treatment] because of an increased fear of malicious use," or by vitiating warranties on the devices.[1950]

ii. Section 117

1) Proposed Class 22: Vehicle Software – Security and Safety Research

As noted above, EFF invokes section 117 in supporting the exemption for vehicle software security research in Class 22. Opponents suggest that proponents have failed to show that all of the proposed activities fall within the narrow categories of use permitted under section 117.[1951] Relying chiefly on the license agreements for entertainment and telematics software identified by proponents in their opening comments, they further assert that proponents have failed to demonstrate under applicable law that vehicle owners own the copy of the computer software that controls the vehicle's ECUs.[1952] They note that proponents rely on the same two cases considered in the 2012

[1947] *Id.* at 8-9.

[1948] AdvaMed Class 27 Opp'n at 5-6 (alleging that in the past proponents used public fear of software insecurities for personal profit).

[1949] *Id.* at 6 ("For this particular exemption, the researchers seek to use the entire portion of the copyrighted work . . . . Courts have typically required small portions of the copyrighted work to be used in order for the use to be considered a fair use. As a result, since the exemption has asked for the use of the entire copyrighted work, this prong points against the use being a fair use of the copyrighted work.").

[1950] *See* Schulman Opp'n at 1; LifeScience Alley Class 25 Opp'n at 4-5.

[1951] *See, e.g.*, Auto Alliance Class 22 Opp'n at 3-6; GM Class 22 Opp'n at 7-10; Global Automakers Class 22 Opp'n at 6; John Deere Class 22 Opp'n at 4-5.

[1952] GM Class 22 Opp'n at 9 (citing EFF Class 22 Supp. at 13-14).

Recommendation, *Krause v. Titleserv, Inc.* and *Vernor v. Autodesk, Inc.*, in which the Register observed the uncertain state of the law regarding ownership of software.[1953] As referenced above, however, opponents conceded at the public hearing for Class 21 that with the exception of the software controlling the entertainment and telematics systems, ECU software is not subject to written licensing agreements.[1954] Opponents did not offer any evidence of ECU license agreements for agricultural equipment.

Opponents also challenge proponents' contention that making copies of computer programs on ECUs is an essential step in the utilization of the computer program in conjunction with a machine and that the copied computer programs are used in no other way.[1955] In opponents' view, proponents cannot demonstrate that security research activities would be limited to what is permitted under section 117, and they specifically note EFF's concession that making copies of vehicle computer programs is "not essential to using the vehicle software for routine driving purposes."[1956] They also dispute that the proposed copying would be for archival purposes as permitted under section 117(a)(2).[1957]

b. Asserted Adverse Effects

i. Proposed Class 25: Software – Security Research

Opponents argue that Class 25 proponents have not demonstrated that the prohibition on circumvention is having, or is likely to have, adverse effects on good-faith security research. According to opponents, "proponents have failed to demonstrate that the prohibition . . . is impeding or chilling legitimate security research activities, including activities falling within the scope of section 1201(j) and other statutory exceptions to the prohibition."[1958]

At the same time, IPO urges that "[i]n view of the vast array of products that could be accessed through the exemption, the public risk [of such research] is impossible

---

[1953] *Id.* at 8-9 (citing *Krause*, 402 F.3d at 124 and *Vernor*, 621 F.3d at 1110-11).

[1954] Tr. at 276:18-24 (May 19, 2015) (Lightsey, GM) ("I think it would be very difficult, if not impossible, to have license agreements covering the myriad of ECU's that are contained in the vehicle.").

[1955] GM Class 22 Opp'n at 10 (citing 17 U.S.C. § 117(a)(1)); *see also* Auto Alliance Class 22 Opp'n at 6; Global Automakers Class 22 Opp'n at 6.

[1956] GM Class 22 Opp'n at 10 (quoting EFF Class 22 Supp. at 15); *see also* Global Automakers Class 22 Opp'n at 6 (Although EFF did not rely on 17 U.S.C. § 117(c), Global Automakers argues that the proposed use of research would not constitute acceptable "maintenance" or "repair" under that provision because it "limits 'maintenance' and 'repair' to those activities aimed at servicing or restoring the automobile to 'work in accordance with its original specifications.'").

[1957] GM Class 22 Opp'n at 10 (citing 17 U.S.C. § 117(a)(2)); *see also* Auto Alliance Class 22 Opp'n at 6 (citing same).

[1958] Auto Alliance Class 25 Opp'n at 1 (citing Auto Alliance Class 22 Opp'n at 9-12); *see also* BSA Class 25 Opp'n at 4; GM Class 25 Opp'n at 12-13; Tr. at 134:15-18 (May 26, 2015) (Lightsey, GM).

to quantify."[1959] BSA expressed particular concern that "proponents seek to circumvent access controls on software that is, for example, crucial to running indispensable programs—such as those associated with the operation of nuclear power plants, medical devices, and automobiles," and asserts that "an exemption that lacks proper safeguards could be disastrous."[1960]

GM argues that none of proponents' examples of supposedly chilled research withstand scrutiny, noting that in the example proponents cite of researchers who received legal threats from Texas Instruments regarding their study of the Data Storage Tag, "the threat [of legal action] had no effect" on the research.[1961] Thus, in GM's view, the alleged chilling effects are more hypothetical than "distinct, verifiable, and measureable."[1962] GM also contends that proponents have not "demonstrated that a significant number of individuals are interested in accessing the software controlling a vehicle's ECUs for the purposes of security research, but [are] hampered from doing so."[1963] GM also questions whether an exemption would lead to the public benefits claimed by proponents, given that at least as of July 2014, the National Highway Traffic Safety Administration ("NHTSA") apparently "was not aware of any instances of consumer vehicle control systems having been hacked."[1964] Similarly, with respect to medical devices specifically, opponents contend that proponents have provided no data that "demonstrates or suggests that allowing open access to protected code would in any way enhance safety or efficacy of [those] devices."[1965]

Opponents additionally maintain that there are alternatives to circumvention that mitigate any potential adverse effects.[1966] In particular, they contend that there is a significant amount of independent security research conducted every day with the encouragement of the affected companies.[1967] Opponents thus argue that obtaining authorization from the software developer or product manufacturer is a viable alternative to circumvention.[1968] For example, AdvaMed asserts that "[e]xisting [FDA] regulations [that] require manufacturers to monitor safe use of devices and take corrective action as

[1959] IPO Class 25 Opp'n at 1.

[1960] BSA Class 25 Opp'n at 2.

[1961] GM Class 25 Opp'n at 14.

[1962] *Id.*

[1963] *Id.*

[1964] *Id.* at 19 (quoting Jim Finkle, *Hacking Experts Build Device To Protect Cars from Cyber Attacks*, REUTERS (July 23, 2014), http://www.reuters.com/article/2014/07/23/us-cybersecurity-autos-idUSKBN0FR2FR20140723).

[1965] AdvaMed Class 25 Opp'n at 8; *see also* MDISS Opp'n at 1.

[1966] *See* AdvaMed Class 25 Opp'n at 8-9.

[1967] BSA Class 25 Opp'n at 4; *see also* Tr. at 130:18-25 (May 26, 2015) (Troncoso, BSA); Tr. at 134:20-135:09 (May 26, 2015) (Lightsey, GM).

[1968] *See, e.g.*, GM Class 25 Opp'n at 13.

appropriate" already lead manufacturers to engage in security research.[1969] LifeScience Alley further contends that "[a]ll major companies in the medical device community are participating with the guidance of the FDA to do research in this area."[1970] In the context of vehicles, GM emphasizes that car manufacturers "partner with third party researchers to identify and address security vulnerabilities," allowing for public open participation where appropriate.[1971]

ii. Proposed Class 22: Vehicle Software – Security and Safety Research

Class 22 opponents challenge the claim that the prohibition on circumvention is having adverse effects. GM notes that proponents "fail[] to identify any real-world occurrences where a car was stolen or attacked as a result of security vulnerabilities or that such an occurrence is likely to occur in the near future."[1972] GM also stresses that proponents "failed to demonstrate substantial vehicle related injury as a result of the current prohibition, noting only one example."[1973] Opponents also contend that proponents "failed to demonstrate that [the prohibition] is impeding or 'chilling' any legitimate research—the main thrust of their argument about adverse effects."[1974] For example, GM contends that EFF has only put forward "anecdotal evidence" of security researchers who are prevented from engaging in research,[1975] and asserts that these "individual cases" are insufficient to meet the rulemaking standard.[1976] Similarly, Auto Alliance asserts that "independent research into the safety and security of computer systems in motor vehicles appears to be a growth business, thriving and even attracting federal government support."[1977] Opponents further contend that there are many alternatives to circumvention for vehicle software security research.[1978] In opponents'

[1969] AdvaMed Class 25 Opp'n at 9.

[1970] LifeScience Alley Class 25 Opp'n at 6.

[1971] GM Class 25 Opp'n at 7-8.

[1972] GM Class 22 Opp'n at 14.

[1973] *Id.* at 15.

[1974] Auto Alliance Class 22 Opp'n at 9.

[1975] GM Class 22 Opp'n at 15; *see also* Auto Alliance Class 22 Opp'n at 11.

[1976] GM Class 22 Opp'n at 15 (citing NOI, 79 Fed. Reg. at 55,690).

[1977] Auto Alliance Class 22 Opp'n at 10-11.

[1978] *See, e.g.*, GM Class 22 Opp'n at 8 ("GM, and other car manufacturers, partner with third party researchers to identify and address security vulnerabilities. In fact, it is quite common for automobile manufacturers to contract with third party testers and researchers for work on various parts of the vehicle."); Auto Alliance Class 22 Opp'n at 11 ("[I]ndependent researchers have an important role to play in flagging potential vulnerabilities, and [the auto industry] works with them in a number of fora to learn about problems they have identified and devise solutions to them. Among these fora are the relevant committees of SAE International . . . . Technical experts from auto manufacturers also participate in major gatherings of 'ethical hackers' such as DEF Con and Black Hat. High levels of industry participation in the annual SAE Battelle Cyber Auto Challenge . . . is further evidence of industry commitment to supporting

view, "[g]iven the availability of programs where manufacturers work with independent researchers to test their products . . . no *substantial* adverse impact occurs as a result of the default 1201 prohibition."[1979]

iii. Proposed Class 27A: Medical Device Software – Security and Safety Research

Class 27A opponents contend that proponents "offer no evidence to support their assertions about the 'risk of the DMCA chilling this form of medical research.'"[1980] According to opponents, "[a]t most the Proponents have inferred that manufacturers will expand their use of TPMs over the next three years."[1981] In opponents' view, such an inference does not meet the "highly specific, strong, and persuasive" evidence standard required to establish that future adverse harm will likely occur within the next three years.[1982] Opponents also maintain that proponents' evidence that independent researchers are currently being harmed by the prohibition on circumvention is either unverified, speculative, or "of the *de minimis* nature that does not meet the rulemaking standard."[1983]

AdvaMed further asserts the proposed exemption is unnecessary, because "[a]lternatives that do not require unauthorized circumvention" exist for medical device software security research.[1984] AdvaMed contends that "medical device manufacturers have been and are presently engaged with technology companies and academic researchers to evaluate the security, safety, and efficacy of medical devices."[1985] In support of this assertion, opponents observe that one medical device manufacturer recently hired three security firms to research the vulnerabilities in a type of insulin pump it produced when it realized the pump was susceptible to attack.[1986] Opponents note that university-affiliated institutions also perform medical device software research with the permission of manufacturers.[1987] They also highlight FDA's recent sponsorship of a public "workshop among industry, academic, and government leaders entitled

---

[alternate means of vehicle software security research]."); John Deere Class 22 Opp'n at 9; Global Automakers Class 22 Opp'n at 7.

[1979] *See* 17 U.S.C. § 1201(a)(1)(A); GM Class 22 Opp'n at 14 (emphasis in original).

[1980] NAM Opp'n at 5 (quoting MDRC Supp. at 20).

[1981] *Id.*

[1982] NOI, 79 Fed. Reg. at 55,690 (quoting STAFF OF H. COMM. ON THE JUDICIARY, 105TH CONG., SECTION-BY-SECTION ANALYSIS OF H.R. 2281 AS PASSED BY THE UNITED STATES HOUSE OF REPRESENTATIVES ON AUGUST 4, 1998, at 6 (Comm. Print 1998)).

[1983] NAM Opp'n at 4-5 (quoting MDRC Supp. at 20).

[1984] AdvaMed Class 27 Opp'n at 7.

[1985] *Id.* at 2.

[1986] *See, e.g.*, IPO Class 27 Opp'n at 2; NAM Opp'n at 6; AdvaMed Class 27 Opp'n at 3.

[1987] *See, e.g., id.*

'Collaborative Approaches for Medical Device and Healthcare Cybersecurity.'"[1988] In light of these alternatives to independent research on medical device software, in opponents' view, "[a]ny alleged research need is purely speculative."[1989]

c. Argument Under Statutory Factors

i. Proposed Class 25: Software – Security Research

Class 25 opponents contend that the statutory factors do not support an exemption. On the first factor, Class 25 opponents assert that "the current availability of legitimate and safe methods of conducting security research" demonstrates that the prohibition does not negatively affect the availability of copyrighted works, emphasizing that companies and manufacturers often voluntarily engage third-party researchers to find and fix software vulnerabilities.[1990] Opponents also contend that the second factor does not weigh in favor of granting an exemption because proponents have provided no evidence that the prohibition has prevented the use of protected software for education purposes, or that there are even a significant number of educational programs focused on teaching security research.[1991] Opponents argue that the third factor also does not weigh in favor of an exemption because proponents have failed to demonstrate on the record that the prohibition has adversely affected legitimate security research, commentary or educational activity.[1992]

On the fourth factor, GM contends that granting an exemption would weaken the security of vehicle safety and emissions systems by allowing the dissemination of highly sensitive information "in an uncontrolled, public environment," and thus would result in a decrease in the value of vehicle software by putting automobile manufacturers "in a position of having to change their security structure, or to consider reducing the availability of advanced systems, each time researchers publish confidential and highly sensitive information about the security structures in place."[1993] GM also argues that having to focus on damage control after sensitive information is publicly disclosed will "detract from [manufacturers'] ability to focus on new and innovative software" and chill investment in developing new ECU software.[1994]

[1988] IPO Class 27 Opp'n at 2; *see also* NAM Opp'n at 6; AdvaMed Class 27 Opp'n at 2-3.

[1989] *See, e.g.*, IPO Class 27 Opp'n at 1.

[1990] GM Class 25 Opp'n at 15-16; *see also* Tr. at 130:10-25 (May 26, 2015) (Troncoso, BSA) (asserting that BSA-member companies "are actively trying to incentivize [independent security research] by offering rewards, either financial or reputational, to those who provide information about security vulnerabilities but do so in a responsible manner").

[1991] GM Class 25 Opp'n at 16-17; *see also* Tr. at 134:15-135:06 (May 26, 2015) (Lightsey, GM).

[1992] *See, e.g.*, GM Class 25 Opp'n at 17 (asserting that, despite the prohibition, articles and papers have been published analyzing and criticizing security systems and potential vulnerabilities in those systems).

[1993] *Id.* at 17-18.

[1994] *Id.* at 18.

Opponents offer various observations addressed to the fifth statutory factor, permitting the Librarian to consider other factors as appropriate. The overall thrust of their concerns is that the proposed exemption should be denied because the risk to public safety that would be created by granting the exemption outweighs the minimal benefits offered by unauthorized security research. For instance, opponents argue that circumvention activities could result in medical device malfunctions that jeopardize safety, particularly in networked medical devices such as implants, and "profoundly change a device's operation resulting in injury or death."[1995] That argument to some degree assumes that medical devices subject to security research would be either in clinical use by patients or ultimately end up in the stream of commerce; as noted above, however, proponents acknowledged that the devices being researched should never be used in patients. Opponents also assert that allowing circumvention without consent of the copyright owner would "encourage malicious actors to access . . . devices and their data without the consent" or knowledge of patients.[1996]

In addition, AdvaMed and other medical device companies assert that an exemption could result in greater products liability suits and increase manufacturers' legal costs because "[a]llowing access to the source code in medical devices without consent and without following the manufacturer's instructions could lead to attacks or misuse that cause medical devices to malfunction."[1997] They also contend that allowing circumvention that exposes a device's source code could "encourage[] theft of trade secrets and the infringement of patents since most source code is either patented or considered to be a trade secret," devaluing innovation in devices and potentially leading to an increase in the number of knock-off products.[1998] According to AdvaMed, an exemption would "create a dangerous precedent likely to be followed by other countries that may see weakening of IP protection as potentially advantageous for indigenous industry focused on imitation rather than innovation."[1999] They also argue that an exemption would result in manufacturers, universities, and other copyright owners investing more of their finite resources into bolstering TPMs and less in "innovation that improves healthcare."[2000]

In addition, opponents argue that an exemption would interfere with the regulatory authority of other federal agencies, as well as other federal and state laws and

---

[1995] AdvaMed Class 25 Opp'n at 3; *see also* LifeScience Alley Class 25 Opp'n at 4; Auto Alliance Class 25 Opp'n at 1 (citing Auto Alliance Class 22 Opp'n at 12-15) (asserting that there are "serious threats to safety and security that recognition of the proposed exemption would create or exacerbate").

[1996] AdvaMed Class 25 Opp'n at 6; *see also* LifeScience Alley Class 25 Opp'n at 4, 6; Tr. at 125:01-05 (May, 26 2015) (Troncoso, BSA).

[1997] AdvaMed Class 25 Opp'n at 5; *see also* LifeScience Alley Class 25 Opp'n at 4.

[1998] AdvaMed Class 25 Opp'n at 5-6; *see also* LifeScience Alley Class 25 Opp'n at 5; Tr. at 132:20-21 (May 26, 2015) (Troncoso, BSA).

[1999] AdvaMed Class 25 Opp'n at 9.

[2000] *Id.* at 5; *see also* MDISS Opp'n at 1 (asserting that allowing circumvention "may adversely impact innovation incentives for universities and companies that create this IP for patients").

regulations. For instance, GM asserts that an exemption could have an "impact on the effectiveness of U.S. regulatory systems for maintaining vehicle safety or emissions if certain information regarding potential security vulnerabilities is publically disseminated and detailed"[2001] and argues that "circumvention of certain emissions-oriented TPMs, such as seed/key access control mechanisms, could be a violation of federal law," including the CAA, which prohibits tampering with vehicles or vehicle engines, or the National Traffic and Motor Vehicle Safety Act, which prohibits introducing non-compliant vehicles into U.S. commerce.[2002]

Opponents similarly assert that allowing the "fixing" of medical devices without FDA or manufacturer permission would risk patient safety because it would "enable others to bypass proper regulatory controls;" they point to the fact that FDA, as the federal agency responsible for assuring the safety, efficacy and security of medical devices, "oversees the design and use of these products with great rigor, and often requires extensive clinical studies to establish safety and efficacy."[2003] AdvaMed argues that allowing circumvention would "increase recall and reporting requirements to FDA," potentially stifling investment in medical technology because manufacturers remain legally "responsible for the safety of their devices even after they have been entered into commerce and altered by a third party."[2004] IPO similarly contends that allowing circumvention and disclosure of software flaws prior to FDA review and approval could put patients "at increased risk from bad faith attempts to modify devices during the period required to develop and obtain [FDA] approval for the change," which can last as long as one to two years.[2005] Citing concerns of patient privacy, MDISS emphasizes that "[i]t's not clear that HIPAA [the Health Insurance Portability and Accountability Act of 1996] supports the access to [protected health information] proposed in this petition."[2006] AdvaMed likewise maintains that an exemption could "contravene federal and state privacy laws concerning the storage and transmission of protected health information"[2007] by potentially compromising such information through unauthorized access or through the exposure of source code and patient data to "inappropriate parties."[2008]

[2001] GM Class 25 Opp'n at 14; *see also* Tr. at 134:06-12 (May 26, 2015) (Lightsey, GM); GM Class 25 Post-Hearing Resp. at 2-3.

[2002] GM Class 25 Opp'n at 6-7; *see also* GM Class 25 Post-Hearing Resp. at 2-3.

[2003] AdvaMed Class 25 Opp'n at 3-5; *see also* IPO Class 25 Opp'n at 1 (noting that "no one should be 'fixing' medical devices or pacemaker applications without [FDA] review and approval . . . . [because t]he risk of patient injury or death is high"); LifeScience Alley Class 25 Opp'n at 2-3.

[2004] AdvaMed Class 25 Opp'n at 4; *see also* LifeScience Alley Class 25 Opp'n at 2 (arguing that "any changes, however insignificant, made to a post market approved device must go through additional screening by the FDA").

[2005] IPO Class 25 Opp'n at 2.

[2006] MDISS Opp'n at 1.

[2007] AdvaMed Class 25 Opp'n at 2.

[2008] *Id.* at 3.

More generally, opponents argue that, to the extent the existing permanent exemptions in sections 1201(f), 1201(g), and 1201(j) are inadequate, the Copyright Office is not the appropriate agency and the 1201 rulemaking proceeding is not the appropriate forum in which to address the issue.[2009] SIIA contends that "[t]o the extent the concerns raised here are legitimate and were not previously raised when [the permanent exemptions] were first enacted, it is for Congress, not the Copyright Office, to determine whether any or all of these three statutory exceptions should be modified."[2010]

Opponents express concern about the potential breadth of the exemption,[2011] and its lack of the reasonable constraints that Congress placed on good-faith security research in section 1201(j).[2012] In addition, MDISS expresses concerns "about the ambiguity of the term 'researcher'" in the proposed exemption, fearing that the exemption could be invoked by a broader range of persons than may be appropriate.[2013] Opponents also argue that the fact that the Librarian previously granted exemptions for security research in 2006 and 2010 should not compel the Librarian to also grant the exemption here, explaining that the 2006 and 2010 exemptions were more narrowly tailored and incorporated "aspects of section 1201(j) to preserve the spirit of Congress' efforts to avoid exacerbating risks"[2014] by limiting the classes to "security testing of CDs and video games that included software where the software itself acted as a TPM and created security flaws and vulnerabilities."[2015] GM additionally argues that the previously granted exemptions are distinguishable because they "had no impact on safety systems, carefully crafted regulatory schemes, or the secure operation of important heavy equipment (like automobiles)."[2016]

As noted above, opponents also express grave concerns about the proper disclosure of vulnerabilities under any exemption. BSA argues that initial disclosure to manufacturers and companies is the "norm," even amongst independent security

[2009] SIIA Class 25 Opp'n at 1 (stating that "it is unnecessary and inappropriate for the Copyright Office to create an exemption for encryption research, security testing or reverse engineering in this triennial rulemaking process"); LifeScience Alley Class 25 Opp'n at 3; *see also* BSA Post-Hearing Resp. at 1.

[2010] SIIA Class 25 Opp'n at 1.

[2011] IPO Class 25 Opp'n at 1 (contending that because the proposed exemption includes a wide range of systems and devices, such as medical devices, car components, supervisory control and data acquisition systems, and other critical infrastructure, "the public risk is impossible to quantify").

[2012] BSA Class 25 Opp'n at 2 (such as being "expressly limited to acts that do not constitute copyright infringement" or violation of other "closely related laws, such as the Computer Fraud and Abuse Act"); *see also* Tr. at 127:19-23 (May 26, 2015) (Troncoso, BSA) (arguing that "proponents are seeking an exemption that is both broader than existing statutory exemptions but which contain none of the important safeguards that Congress deemed important"); BSA Post-Hearing Resp. at 2-3.

[2013] MDISS Opp'n at 1.

[2014] BSA Class 25 Opp'n at 3.

[2015] GM Class 25 Opp'n at 19-20; *see also* Tr. at 136:03-11 (May 26, 2015) (Troncoso, BSA).

[2016] GM Class 25 Opp'n at 21.

researchers.[2017] In that regard, BSA observes that in all the examples of independent security research relied upon by proponents, the research results were voluntarily disclosed to the companies before being publicly disclosed.[2018] Opponents argue that if the exemption does not impose a disclosure standard, it will allow "researchers to make disclosures about vulnerabilities based upon the researcher's sole judgment before the software developer or product manufacturer has had an opportunity to remedy the problem."[2019] Opponents argue that such an exemption would therefore "authorize the public disclosure of security vulnerabilities in ways that would expose the public to heightened security risks," especially in the case of public disclosure of vulnerabilities "concurrent" with disclosure to the software developer or product manufacturer.[2020] GM further asserts that, in the case of vehicles, even a requirement of prior disclosure to the manufacturer "would create safety and security risks," because "many vehicle owners do not participate in the fixes auto manufacturers already offer when recalls issue."[2021] In the context of medical devices, IPO has concerns with public disclosure in and of itself, arguing that patients who have implanted devices, such as implantable pacemakers, "will be placed at risk from public disclosure for the remaining lifetime of their implanted devices, which may be as much as 15 years."[2022]

At the same time, opponents also appear opposed to the Office's endorsement of specific disclosure practices, instead preferring an approach to disclosure that tracks section 1201(j), which prescribes a multifactor standard to assess disclosure in any given instance.[2023] Opponents note the First Amendment concerns that could be implicated by

[2017] Tr. at 153:04-154:05 (May 26, 2015) (Troncoso, BSA).

[2018] *Id.*

[2019] *Id.* at 125:11-17 (Troncoso, BSA); *see also id.* at 135:10-16 (Lightsey, GM) (expressing concerns that "the ability for automobile manufacturers to control that research and to have the opportunity to fix vulnerabilities before they're widely disclosed would be severely limited and could thus create safety concerns"); GM Class 25 Opp'n at 6 (asserting that allowing circumvention "increases access to, and as noted by Proponents, *publication* of sensitive information relating to the operation of ECUs which in turn increases the risks to safety and security and other systems that an owner trusts"); BSA Post-Hearing Resp. at 1.

[2020] BSA Class 25 Opp'n at 2 (pointing with concern to software "associated with the operation of nuclear power plants, medical devices, and automobiles"); *see also id.* at 5; Tr. at 128:23-129:07 (May 26, 2015) (Troncoso, BSA) (noting that "there is already a thriving market . . . in the black market for security research regarding zero day vulnerabilities"); Tr. at 125:21-126:01 (May 26, 2015) (Troncoso, BSA) (arguing that an exemption would "enable exploitation of vulnerabilities to engage in identity theft, financial fraud, and other serious threats to our nation's critical infrastructure"); BSA Post-Hearing Resp. at 1; GM Class 25 Post-Hearing Resp. at 1-2.

[2021] GM Class 25 Post-Hearing Resp. at 2.

[2022] IPO Class 25 Opp'n at 2.

[2023] 17 U.S.C. § 1201(j)(3); *see* BSA Post-Hearing Resp. at 3.

any disclosure requirement, and the fact that the appropriate timing of disclosure to companies and manufacturers may differ based on the nature of the vulnerability.[2024]

ii. Proposed Class 22: Vehicle Software – Security and Safety Research

Regarding the first statutory factor, Class 22 opponents argue that the proposed exemption is unnecessary, and would not increase the availability of copyrighted works. Specifically, opponents argue vehicle software is already commercially available for use, subject to the conditions of applicable licenses or vehicle sales agreements.[2025] Opponents further assert that the prohibition will not decrease the availability of vehicle software for research purposes, because alternate means of examining vehicle software for security research are already in place without an exemption.[2026]

With respect to the second factor, opponents generally maintain that the proposed exemption by definition would not enhance the availability for use of works for nonprofit archival, preservation, and educational purposes.[2027]

Opponents present little argument regarding the third factor. Opponents do not deny that the proposed exemption, focusing on security research for vehicle software, categorically falls under "research," something to be examined under the third factor.[2028] But opponents argue that the proposed exemption would disrupt and undermine auto manufacturers' own legitimate efforts to conduct security research into their vehicle software.[2029]

Turning to the fourth factor, the effect of circumvention on the market for or value of the works, Auto Alliance argues that proponents "are wrong to assert that allowing unrestricted circumvention of access controls protecting [vehicle software] code will

---

[2024] BSA Post-Hearing Resp. at 3; Tr. at 131:08-132:01 (May 26, 2015) (Troncoso, BSA); GM Class 25 Post-Hearing Resp. at 2. BSA also highlights that the U.S. government is currently addressing disclosure of vulnerability information with special focus on avoiding unintended consequences, pointing to the Administration's contemplation of policy initiatives on the issue and the Department of Commerce's consideration of export controls on tools used to hack and discover vulnerabilities. Tr. at 126:08-127:03 (May 26, 2015) (Troncoso, BSA); *see also* BSA Post-Hearing Resp. at 1-2.

[2025] John Deere Class 22 Opp'n at 12.

[2026] GM Class 22 Opp'n at 16 ("With regard to software glitches 'many companies pull in an external source code inspector to preemptively catch and remove the bugs.' Manufacturers also contract with researchers. These arrangements can be open to public participation, such as with many standard setting organizations, or may be confidential, when sensitive information about TPMs and operation of ECUs is required for appropriate research or evaluation."); Global Automakers Class 22 Opp'n at 5-6 ("[A]utomobile manufacturers . . . are well under way with their own internal and external research programs.").

[2027] John Deere Class 22 Opp'n at 12; GM Class 22 Opp'n. at 10.

[2028] *See* 17 U.S.C. § 1201(a)(1)(C)(iii); *see, e.g.*, John Deere Class 22 Opp'n at 12-13.

[2029] *See, e.g.*, John Deere Class 22 Opp'n at 12-13; Global Automakers Class 22 Opp'n at 7; GM Class 22 Opp'n at 17.

produce 'no market harm cognizable by copyright law.'"[2030] GM posits that "the value of the vehicle software will likely decrease as OEMs [original equipment manufacturers] are continually put in a position of having to change their security structure, or to consider reducing the availability of advanced systems, each time researchers publish confidential and highly sensitive information about the security structures in place."[2031] GM further asserts that this devaluation of vehicle software resulting from the proposed exemption will have "chilling effects on OEMs' investment in the development of new ECU software,"[2032] and the publication of sensitive security information will hamper manufacturers' efforts to create innovative vehicle software.[2033] GM also argues that the proposed exemption will depress the value of copyrighted works in used vehicles, because consumers in the secondary market will not know when vehicle software has been altered undesirably.[2034]

Regarding the fifth statutory factor, which permits consideration of such other factors as the Librarian deems appropriate, opponents argue that the proposed exemption threatens public safety, because publication of vehicle software research results could facilitate illegal activities.[2035] Opponents also urge that the proposed exemption will "greatly increase risks to the safety and security of every American motorist, passenger, and pedestrian,"[2036] because altering vehicle computer programs can unintentionally compromise critical safety systems.[2037] Opponents additionally assert that the proposed exemption would facilitate noncompliance with industry safety standards and with federal environmental emissions regulations.[2038] Opponents contend that the proposed exemption contradicts Congress's intent in enacting section 1201(j), which

---

[2030] Auto Alliance Class 22 Opp'n at 15 (citing EFF Class 22 Supp. at 23).

[2031] GM Class 22 Opp'n at 17.

[2032] *Id.*

[2033] *Id.*

[2034] John Deere Class 22 Opp'n at 8 ("Consumers looking to purchase a used car will be fearful that the previous owner could have tinkered with or hacked the vehicle in ways that could cause it to perform in unexpected ways, or, worse, have introduced viruses and malware into the vehicle's systems."); Global Automakers Class 22 Opp'n at 8 ("The proposed exemption . . . gambles with the value of used automobiles to downstream purchasers.").

[2035] *See, e.g.*, Auto Alliance Class 22 Opp'n at 14 ("EFF's submission details a long list of reported vulnerabilities whose exploitation could directly threaten driver, passenger and public safety as well as privacy."); Global Automakers Class 22 Opp'n at 2 ("The very real risk that ostensibly legitimate research unwillingly undermines vehicle security by serving as a guidebook to software vulnerabilities that enables or even accelerates illicit hacking and malicious modifications to automotive software weighs heavily against the proposed exemption.").

[2036] Auto Alliance Class 22 Opp'n at 13.

[2037] Global Automakers Class 22 Opp'n at 4 ("Intentions aside, even well-meaning research and slight modifications in the name of security could cause entire systems to malfunction.").

[2038] *See, e.g.*, GM Class 22 at 5 ("[C]ircumvention of certain emissions-oriented TPMs, such as seed/key access control mechanisms could be a violation of federal law."); John Deere Class 22 Opp'n at 18-22; Global Automakers Class 22 Opp'n at 6.

"communicates a strong Congressional bias toward prudence and caution in disclosing [security research] results, lest the disclosure degrade the security of all current and future users of that system or network."[2039] In sum, opponents argue that "this proposal presents one of those circumstances . . . in which the balance of harms counsels rejection."[2040]

iii. Proposed Class 27A: Medical Device Software – Security and Safety Research

Concerning the first statutory factor, Class 27A opponents contend that the availability for use of medical device software for research purposes is not currently being impeded by the prohibition on circumvention.[2041] According to NAM, "[m]anufacturers have both the incentive to ensure the security and stability of their products and demonstrated records of making their copyrighted computer programs available for research, analysis, and testing by qualified independent parties."[2042]

Opponents present limited argument with respect to the second factor, although they suggest that the availability for use of medical device software for nonprofit educational purposes will not be hampered by the prohibition, because medical device software research is already taking place at public university-affiliated research institutions.[2043]

With respect to the third factor, opponents contend that the prohibition on circumvention does not negatively impact the public's ability to use copyrighted works for teaching, scholarship, or research.[2044] To support this assertion, opponents reference research occurring at university-affiliated institutions, in the private sector, and through government-sponsored collaborations.[2045] Opponents also maintain that the prohibition on circumvention is not currently hampering commentary, criticism, or reporting on medical devices.[2046]

[2039] Auto Alliance Class 22 Opp'n at 13; *see also* 17 U.S.C. § 1201(j).

[2040] Auto Alliance Class 22 Opp'n. at 12.

[2041] *See, e.g.*, IPO Class 27 Opp'n at 1.

[2042] NAM Opp'n at 3.

[2043] *See, e.g.*, LifeScience Alley Class 27 Opp'n at 3 (highlighting the University of Minnesota's Technological Leadership Institution Project); AdvaMed Class 27 Opp'n at 3 (noting the Archimedes Institute at the University of Michigan focuses on medical device security).

[2044] NAM Opp'n at 6.

[2045] *See, e.g., id.*

[2046] LifeScience Alley Class 27 Opp'n at 3 (stating collaborative research on the security of medical device software conducted at the University of Minnesota's Technological Leadership Institute in partnership with the National Cybersecurity Center of Excellence at the National Institute of Standards and Technology is to include formal release for public comment).

As for the fourth factor, opponents assert that the proposed exemption would harm the market for or value of medical device software, because any alterations to the computer programs made by independent researchers will nullify the device's warranty and "may result in an increase in cost of the device."[2047] LifeScience Alley contends that unauthorized circumvention alone, absent changes to the medical device computer programs, "would be outside of the manufacture's design, potentially voiding any warranty associated with the device."[2048] LifeScience Alley maintains that circumvention conducted by independent researchers "could expose the manufacturer to unforeseeable liability."[2049] Opponents also opine that the proposed exemption would harm the market for medical device software, because independent researchers "could jeopardize the security of implanted devices" in the course of conducting legitimate security research.[2050] Finally, opponents contend that unauthorized circumvention and independent research conducted by unqualified device users may result in publicized device failures, thereby reducing market demand.[2051]

In terms of other factors that the Librarian should consider, LifeScience Alley asserts that the proposed exemption contravenes FDA's recommended cybersecurity policy for medical device software; according to LifeScience Alley, FDA's guidelines recommend that medical device manufacturers "limit access to the devices to trusted users only," while the exemption would allow unauthorized access to devices.[2052] Opponents observe that "[t]he FDA is charged with ensuring [medical devices] are safe and effective, and . . . the agency has taken a keen interest in cyber-security." They thus urge the Office to "solicit and consider the FDA's views" in considering the proposed exemption.[2053]

3. Discussion

Based on the entirety of the record and as set forth below, the Register concludes that proponents have demonstrated that good-faith testing for and the identification, disclosure and correction of malfunctions, security flaws and vulnerabilities in copyrighted computer programs have been hindered by TPMs that protect those programs. The Register further concludes that the existing permanent exemptions in section 1201 do not cover the full range of proposed security research activities, many of which proponents have established are likely be noninfringing. In addition, on the

[2047] *See, e.g., id.* at 5.

[2048] *Id.* at 4.

[2049] *Id.*

[2050] *See, e.g.*, NAM Opp'n at 7-8; IPO Class 27 Opp'n at 1; AdvaMed Class 27 Opp'n at 7.

[2051] *See e.g.*, NAM Opp'n at 7 ("[T]he proliferation of device failures could have the unintended consequence of deterring patients from utilizing these life-saving technologies.").

[2052] LifeScience Alley Class 27 Opp'n at 2 (citing FDA PREMARKET SUBMISSION GUIDANCE).

[2053] IPO Class 27 Opp'n at 2-3.

whole—though with important qualifications—the Register finds that the statutory factors set forth in section 1201(a)(1) tend to favor proponents.

a. Noninfringing Uses

As explained above, the three proposed security-related exemptions for general software security research, vehicle software security research, and medical device software security research are to some extent overlapping and have common legal underpinnings. Given this relationship among the proposed classes, the Register concludes that it is appropriate to consolidate the analysis and recommendations for these three classes.

The Register finds that the overall record supports proponents' claim that accessing and reproducing computer programs for purposes of facilitating good-faith security research and identification of defects are likely to be fair uses of the programs under section 107. With respect to the proposed exemption for vehicle software security research in Class 22, the Register additionally finds that these uses may qualify as noninfringing under section 117 as well, at least in some circumstances. The Register notes that proponents did not raise section 117 in the other two security-related classes, and thus expresses no view on its applicability in those contexts.

i. Fair Use

Regarding the first fair use factor, the record establishes that the purpose and character of the proposed uses tend to support a finding of fair use. Many of the proposed uses in the three security research classes are likely to be transformative, including copying the work to perform testing and research.[2054] In many cases the purpose of the use is to engage in academic inquiry.[2055] The desired research activities may result in criticism or comment about the work and the devices in which it is incorporated, including potential flaws and vulnerabilities.[2056] As explained in the record, the goal of good-faith security research is "to educate the public . . . about these risks and how to mitigate them."[2057] Thus, in many cases, research activities may also extend to evaluating and describing how to fix flaws that have been discovered.[2058]

Accordingly, good-faith security research encompasses several of the favored activities listed in the preamble of section 107.[2059] As the Register stated in the 2010

[2054] *See, e.g.*, Green Class 25 Supp. at 15-17; EFF Class 22 Supp. at 7; MDRC Class 27 Supp. at 13.

[2055] Tr. at 47:02-09 (May 26, 2015) (Bellovin).

[2056] *See, e.g.*, *id.* at 74:09-15 (Blaze); *id.* at 47:02-09 (Bellovin).

[2057] EFF Class 22 Supp. at 8.

[2058] Green Class 25 Supp. at 11 (noting that "[a]pplying research discoveries to fix vulnerabilities or build new, more secure software and devices" is "part of the overarching, holistic process of engaging in 'security research'").

[2059] 17 U.S.C. § 107 (listing purposes of "criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research").

Recommendation regarding an exemption for good-faith security testing of video games, "socially productive, transformative uses performed solely for good faith testing, investigation . . . of security flaws or vulnerabilities weigh heavily in favor of fair use under the first factor."[2060] Therefore, the Register finds that, on the current record, the first factor is generally favorable to proponents.

The second factor, the nature of the work, also favors proponents. As explained above, the proposed classes focus on software embedded in or otherwise used in consumer-facing devices. When a computer program is being used to operate a device, the work is likely to be largely functional in nature, as in the case of a cellphone's operating system, software contained in a vehicle's ECU, or software used to control a medical device. On the facts presented here, for purposes of fair use, the computer programs at issue are likely to fall on the functional rather than creative end of the spectrum.[2061]

In addressing the third factor, which considers the amount of the work used, proponents concede that in most cases the proposed uses would involve reproduction of copyrighted computer programs in their entirety.[2062] Courts have been willing to permit complete copying of the original work, however, where it is necessary to accomplish a transformative purpose.[2063] Furthermore, where functional elements of a computer program cannot be investigated or assessed without some intermediate reproduction of the works, courts have held that the third factor is not of significant weight.[2064] And in prior rulemakings, the Register has found such copying to be consistent with fair use, for example, in granting exemptions for good-faith security research into compact discs during the 2006 proceeding, and for security research into video games during the 2010 proceeding.[2065] Thus, while the third factor arguably disfavors a fair use finding, the weight to be given to it under the circumstances is slight.

Factor four is concerned with market impact, and evaluates "not only the extent of market harm caused by the particular actions of the [user], but also 'whether unrestricted and widespread conduct of the sort engaged in by the [proponent of fair use] . . . would result in a substantially adverse impact on the potential market.'"[2066] Proponents persuasively establish that the desired security research will not usurp the market for any

[2060] 2010 Recommendation at 184.

[2061] *See Sega*, 977 F.2d at 1524 (reaching a similar conclusion regarding reproductions of video games for purposes of reverse engineering the code and enabling interoperability).

[2062] *See, e.g.*, EFF Class 22 Supp. at 10.

[2063] *Authors Guild, Inc. v. HathiTrust*, 755 F.3d 87, 98 (2d Cir. 2014) ("For some purposes, it may be necessary to copy the entire copyrighted work, in which case Factor Three does not weigh against a finding of fair use."); *Kelly v. Arriba Soft*, 336 F.3d at 820-21 (holding that the third fair use factor did not weigh against copier when entire-work copying was reasonably necessary).

[2064] *Sega*, 977 F.2d at 1510.

[2065] 2006 Final Rule, 71 Fed. Reg. at 68,477; 2010 Final Rule, 75 Fed. Reg. at 43,832-33.

[2066] *Campbell*, 510 U.S. at 590.

original works subject to that research, as they will be lawfully obtaining copies of those works for analysis.[2067] Proponents also persuasively establish that any market harm resulting from independent researchers would be due to potential criticism resulting from the research, which is not considered a cognizable harm under the fourth factor.[2068] As explained by the Supreme Court in *Campbell v. Acuff-Rose Music, Inc.*, "there is no protectible derivative market for criticism."[2069]

The Register further finds that opponents' arguably speculative concerns regarding reputational harms do not tip the scales in opponents' favor. Ultimately, the expressed reputational concerns largely amount to a desire to avoid negative publicity before a device manufacturer is able to address a discovered flaw. While such concerns may result in market harm, this type of reputational harm is not the concern of copyright.[2070] It is also worth noting that in some cases, the product manufacturer may benefit by making the product more reliable, and hence valuable, in response to a discovered flaw. Thus, the Register finds that, on the current record, the fair use analysis under the fourth factor tends to favor proponents.

Although in the context of Class 21, which concerns access to vehicle software for purposes of diagnosis, repair, and modification, the Register found that the fair use analysis did not support extending the exemption to computer programs that are chiefly designed to operate vehicle entertainment and telematics systems, a different conclusion is warranted here. In Class 21, discussed above, proponents focused principally on the ability to circumvent TPMs on the ECUs that are used to operate the vehicle mechanically, and the record did not support the need to access the entertainment and telematics systems for purposes of vehicle diagnosis, repair, or modification.[2071] Here, in contrast, the record demonstrates a strong need to research the computer programs in entertainment and telematics systems; indeed, the evidence shows that previous research into those systems has uncovered flaws that can be used to affect a vehicle's operation as a whole.[2072] Moreover, opponents' concerns under Class 21 that access to entertainment

---

[2067] *See, e.g.*, Green Class 25 Supp. at 17; CDT Reply at 5-6 (quoting 2010 Recommendation at 186); *see also* Green Class 25 Reply at 9; MDRC Supp. at 12 (citing *Cariou v. Prince*, 714 F.3d at 708-09).

[2068] *See, e.g.*, EFF Class 22 Reply at 7-8; Green Class 25 Supp. at 17; MDRC Supp. at 12 (citing *New Era v. Carol Publ'g*, 904 F.2d at 160; *Wojnarowicz v. Am. Family Ass'n*, 745 F. Supp. at 145-46; 2012 Recommendation at 73).

[2069] *Campbell*, 510 U.S. at 592.

[2070] *Id.*

[2071] *See, e.g.*, EFF Class 21 Supp. at 6-7 (describing uses covered by the Class 21 exemption); Auto Alliance Class 21 Opp'n at 15 n.65 (noting that proponents' submissions "make virtually no reference to [telematics] services").

[2072] *See* Tr. at 16:11-23 (May 19, 2015) (Miller) (noting research showing "several vulnerabilities in [a] vehicle, for example, the Bluetooth stack and the cellular components—think OnStar, for example—that allowed them to inject . . . messages into a vulnerable vehicle anywhere in the country" and "remotely lock[] up the brakes on these vehicles or cause other safety critical [flaws]"). GM's witness testified that "[v]ehicles' ECUs are interconnected by a network that enable interaction between various systems and/or telematics equipped vehicles with various remote features." *Id.* at 26:13-16 (Lightsey, GM).

and telematics ECUs for purposes of repair and modification could also be exploited to gain unauthorized access to the content on entertainment systems or subscription telematics services are considerably less forceful in the security context.[2073] Although Class 22 opponents argue that the exemption for security research could also be used to gain unauthorized access to creative content,[2074] the nature and context of security research—as opposed to vehicle modification—would appear to create less of a risk that the exemption would be exploited for this type of unlawful purpose.

On balance, the fair use analysis demonstrates that many of the proposed uses are likely to be socially productive and fair.

ii. Section 117

1) Proposed Class 22: Vehicle Software – Security and Safety Research

In the context of the vehicle software security exemption in Class 22,[2075] proponents have also suggested that section 117 may apply because the making of copies and adaptations of computer programs is a required step in the security testing process.[2076] Section 117 requires consideration of two questions: whether the person who possesses the machine or device is the owner of the embedded computer program, and whether creating a new copy or adaptation is an essential step in the utilization of the computer program with the machine.

In past rulemaking proceedings, the Register has reviewed the relevant case law governing the determination of ownership of a software copy for purposes of section 117 when formal title is lacking and/or a license or agreement imposes restrictions on the use of the computer program, and has concluded that the law is less than clear.[2077] While the two leading precedents, *Vernor v. Autodesk, Inc.*[2078] and *Krause v. Titleserv, Inc.*,[2079] offer "useful guideposts," these cases are "controlling precedent in only two circuits and are inconsistent in their approach."[2080]

[2073] *See* GM Class 21 Post-Hearing Resp. at 1-2.

[2074] Auto Alliance Class 21 Post-Hearing Resp. at 1.

[2075] In Classes 25 and 27A, the record did not include any meaningful analysis regarding the application of section 117.

[2076] *See, e.g.*, EFF Class 22 Reply at 8-11.

[2077] *See* 2010 Recommendation at 90 (noting that "the law relating to who is the owner of a copy of a computer program under [s]ection 117 is in flux"); 2012 Recommendation at 92 ("The Register concludes that the state of the law remains unclear.").

[2078] 621 F.3d 1102.

[2079] 402 F.3d 119.

[2080] 2012 Recommendation at 92.

In *Krause*, the Second Circuit held that formal title is not necessary to demonstrate ownership under section 117, and that courts should instead look to a variety of factors to determine "whether the party exercises sufficient incidents of ownership over a copy of the program to be sensibly considered the owner of the copy."[2081] These factors include: "(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."[2082] By contrast, in *Vernor*, the Ninth Circuit held that "a software user is a licensee rather than an owner of a copy, where the copyright owner (1) specifies that the user is granted a license; (2) significantly restricts the user's ability to transfer the software; and (3) imposes notable use restrictions."[2083] These tests remain the two dominant approaches to the question of whether software is owned or licensed.

But under either test, the record here supports the conclusion that vehicle owners may well own the ECU computer programs, with the possible exception of certain entertainment and telematics systems that are subject to written licenses. Beyond such discrete license agreements, opponents offered little evidence to support the notion that embedded vehicle software is licensed rather than owned by its users.[2084] Opponents point to no restrictions on owners' use or resale of the relevant computer programs when they transfer the vehicles that contain them.[2085] Thus, based on the record, it appears that some portion of vehicle owners would qualify as "owners" of the relevant computer programs under applicable precedent, at least with regard to computer programs that are not chiefly designed to operate vehicle entertainment or telematics systems.

The record further shows that reproduction and alteration of computer programs is often an "essential step" in the process of identifying potential flaws.[2086] In order to understand the functionality of a computer program, one may need to make a copy to use it in conjunction with a "machine," such as a general-purpose computer, on which the

[2081] *Krause*, 402 F.3d at 124.

[2082] *Id.*

[2083] *Vernor*, 621 F.3d at 1111.

[2084] Tr. at 183:02-12 (May 19, 2015) (Walsh, EFF).

[2085] *See, e.g.*, EFF Class 22 Reply at 9-10.

[2086] *See, e.g., id.* at 10.

program will be analyzed.[2087] This would thus appear to meet the requirements of section 117(a)(1).[2088]

Additionally, proponents have established that the creation of backup copies of computer programs may be important for security research—whether to serve as a baseline for comparison during experiments, or to restore a vehicle ECU to its original state after research is completed. These activities may well be covered by the provision permitting creation of archival-purpose copies, addressed in section 117(a)(2).[2089] Based on the record submitted, then, it is therefore likely that many of the security research uses proposed for owners of vehicles may qualify as protected uses under section 117.

Last but not least, the Register notes that regardless of whether research technically qualifies as noninfringing under section 117, that provision highlights Congress's general view of the importance of users' ability to copy and adapt the computer programs they own to enhance their usefulness, and reinforces the conclusion that such uses here are likely to be fair.[2090]

b. Adverse Effects

Based on the overall record in this proceeding, the Register concludes that TPMs protecting computer programs have a substantial adverse impact on good-faith testing for and the identification, disclosure and correction of malfunctions, security flaws and vulnerabilities in the protected computer programs.[2091]

Proponents argue, and opponents do not dispute, that a significant number of product manufacturers employ TPMs on computer programs.[2092] Proponents establish in the record that in many instances these TPMs have an adverse impact on the ability to engage in security research.[2093] Although opponents have shown that significant independent research is taking place through the cooperation of copyright owners and

---

[2087] *See* EFF Class 22 Supp. at 15.

[2088] *See* 17 U.S.C. § 117(a)(1) (requiring that the "a new copy or adaptation [be] created as an essential step in the utilization of the computer program in conjunction with a machine and that it [be] used in no other manner").

[2089] *See id.* § 117(a)(2) (requiring that the "new copy or adaptation [be] for archival purposes only").

[2090] *See also id.* § 1201(f) (permanent exemption from anticircumvention provisions of section 1201 for reverse engineering activities).

[2091] As noted above, although the proposals referenced databases in addition to computer programs, no evidence was presented demonstrating a need to access databases for purposes of security research, and the exemption does not extend to databases.

[2092] *See, e.g.*, Green Class 25 Pet. at 2-3; Green Supp. at 5-11; Bellovin et al. Pet. at 5; EFF Class 22 Supp. at 4-6; MDRC Supp. at 7-9.

[2093] Green Class 25 Supp. at 17-18; *see also* CDT Supp. at 3; Radcliffe Supp. at 1; Rice Supp. at 1; Stanislav Supp. at 1; USACM Supp. at 1; Green Class 25 Reply at 4; Tr. at 20:08-23 (May 26, 2015) (Green); Tr. at 38:01-20 (May 26, 2015) (Sayler on behalf of Green); Tr. at 40:24-42:04 (May 26, 2015) (Stanislav, Rapid7); Tr. at 71:01-08 (May 26, 2015) (Matwyshyn).

manufacturers,[2094] proponents convincingly argue that adverse effects persist despite the existence of authorized research. For example, there is substantial evidence that the DMCA prohibition continues to discourage academic institutions and government entities from funding critical security research due to uncertainty about the legality of the circumvention that may be involved.[2095] Furthermore, the record establishes that there are significant shortcomings to pursuing research in concert with software developers and product manufacturers, who may have reason to delay publication of research results or prevent public disclosure of vulnerabilities.[2096]

The record reveals a variety of research projects across Classes 25, 22 and 27A that could implicate the circumvention prohibition in section 1201(a)(1) and thus be foreclosed absent an exemption. As previously noted, however, these examples largely focused on consumer-oriented software and devices. For example, Class 25 proponents seek to research the security of a growing number of internet-enabled consumer goods, such as webcams, smoke alarms, and security cameras. [2097] At the hearing, there was focus on a Wi-Fi-enabled voicemail device designed for children that was vulnerable to hacking by strangers.[2098] Proponents also expressed the desire to research electronic voting machines to assess the potential for tampering.[2099]

Proponents of Class 25 failed to explain, however, how the prohibition on circumvention is adversely affecting security research into computer programs that control critical components of the nation's infrastructure, such as nuclear power plants, smartgrids, industrial control systems, air traffic control systems, train systems, and traffic lights. Nor do proponents explain why research into critical systems is not being or could not be conducted with the authorization of the relevant copyright owner.

Under Class 22, which focuses on vehicle software, the record also establishes that section 1201(a)(1) is likely to chill independent research, as some researchers appear not to be pursuing analysis of vehicle software out of fear of legal liability.[2100] The record further indicates that allowing more research could help automobile buyers make more informed purchasing decisions and encourage manufacturers to produce more secure software.[2101]

[2094] BSA Class 25 Opp'n at 4; *see also* Tr. at 130:18-25 (May 26, 2015) (Troncoso, BSA); Tr. at 134:20-135:09 (May 26, 2015) (Lightsey, GM).

[2095] *See, e.g.*, CDT Reply at 6-8.

[2096] *See, e.g., id.* at 7-8; Schneier Class 25 Reply at 1-2; Tr. at 159:06-160:22, 204:21-205:09 (May 26, 2015) (Bellovin).

[2097] Bellovin et al. Supp. at 9; Green Class 25 Supp. at 12.

[2098] Tr. at 41:03-08 (May 26, 2015) (Stanislav, Rapid7).

[2099] VVF Supp. at 1; Tr. at 72:11-20 (May 26, 2015) (Blaze).

[2100] Tr. at 45:08-13 (May 19, 2015) (Charlesworth, USCO; Miller).

[2101] EFF Class 22 Supp. at 16; Schneier Class 22 Reply at 2 ("When researchers are not free to disclose their findings, companies are free to ignore them . . . . If we expect the market to motivate manufacturers to

A similar conclusion is warranted under Class 27A, covering research into medical device software. The record indicates that, in the past, independent security research on medical device software did not typically implicate anticircumvention law because medical devices did not typically employ TPMs.[2102] But there is clear evidence that this is changing as manufacturers begin to employ TPMs, especially in response to FDA guidance encouraging them to do so. Accordingly, the record establishes that legitimate independent research could be impeded as medical devices become subject to section 1201(a)(1).[2103]

Additionally, proponents make a compelling case that the current permanent exemptions in section 1201, specifically section 1201(f) for reverse engineering, section 1201(g) for encryption research, and section 1201(j) for security testing, are inadequate to accommodate their intended purposes.[2104]

Section 1201(f) permits circumvention for the "sole purpose" of identifying and analyzing elements of computer programs necessary to achieve interoperability.[2105] Security research does not, however, always have as its sole purpose the enabling of computer program interoperability, and is often directed at other purposes, such as exposing and correcting security flaws.[2106]

Section 1201(g) addresses efforts to advance encryption technologies,[2107] but the record establishes that security research does not always involve encryption technologies. Moreover, section 1201(g) requires researchers to attempt to obtain authorization from copyright holders, and this may not always be feasible.[2108]

The permanent exemption for security testing in section 1201(j) is closer to the subject of the exemptions requested in Classes 22, 25, and 27A, in that the provision is intended to permit "good faith testing, investigating, or correcting" of "security flaw[s] or

---

design secure products, there must be consumer-advocate testing and evaluation so that users can make intelligent buying decisions.").

[2102] MDRC Supp. at 3, 19-20; MDRC Reply at 2-3.

[2103] *See* 17 U.S.C. § 1201(a)(1)(A); MDRC Supp. at 20; *see also, e.g.*, Schneier Class 27 Supp. at 2; Green Class 27 Supp. at 1; Public Knowledge Class 27 Reply at 5.

[2104] Proponents also mention in passing that the permanent exemption embodied in section 1201(e) does not meet their needs. Section 1201(e) allows "lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State." 17 U.S.C. § 1201(e). This provision thus allows private security researchers to conduct research for one of the listed purposes at the behest of the government through a contractual arrangement, but does not extend to privately initiated research, which is the focus of Classes 25, 22 and 27A.

[2105] *Id.* § 1201(f).

[2106] Green Class 25 Supp. at 19-20.

[2107] 17 U.S.C. § 1201(g).

[2108] *See, e.g.*, Green Class 25 Supp. at 20.

vulnerabilit[ies]" in computer systems.[2109] The Register nonetheless agrees with proponents that this provision is inadequate for several reasons. First, it is not entirely clear whether the exemption is intended to apply where a researcher is not seeking to gain access to "a computer, computer system, or computer network," but instead to software that runs on a device such as an automobile or a medical device.[2110]

As the Register framed similar concerns in 2006, the issue is whether the permanent exemption in 1201(j) is of "insufficient scope because it addresses accessing computers, not access to works, and . . . the proponents seek access to works."[2111] In addressing concerns regarding the scope of 1201(j) in 2006, the Register concluded:

> 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 [to conduct research on copy-protected compact discs], the Register cannot conclude that it is unnecessary to consider an exemption for the proposed class of works.[2112]

The Register reiterated this uncertainty in 2010, finding that the same question and conclusion were called for when the exemption sought access to video games.[2113] As the Register explained then, in enacting section 1201(j), Congress "appeared to be addressing firewalls and antivirus software that were used on computers, computer systems and networks to protect their respective contents," and "wanted to encourage independent evaluation of such security systems."[2114] Given that understanding of Congress's intent, the Register concluded that the proposed exemption for video games did not clearly fall within section 1201(j). Similarly, here, the Register finds that there is some uncertainty regarding whether section 1201(j) encompasses security research that is primarily focused on testing and identifying flaws in computer programs rather than security systems that protect computer systems. Although the security research encompassed by the proposed exemptions may take place *on* a computer, it may not necessarily involve *accessing* a computer as that term is used in section 1201(j).

[2109] 17 U.S.C. § 1021(j).

[2110] Green Class 25 Supp. at 21 (citing 2010 Final Rule, 75 Fed. Reg. at 43,832-33).

[2111] 2006 Recommendation at 59.

[2112] *Id.*

[2113] 2010 Recommendation at 200.

[2114] *Id.* at 196.

Second, section 1201(j) requires that security testing take place "with the authorization of the owner or operator of the computer, computer system, or computer network."[2115] In some cases, it may be difficult to identify the relevant owner, such as when the focus of the research is on general-purpose software that runs on a wide range of devices, or where the owner of software on a particular device is not known.[2116] Moreover, it may not be feasible to obtain authorization even where there is an identifiable owner.

Finally, the Register notes that the multifactor standard in section 1201(j) may be difficult to apply to the proposed uses here. These factors include whether the information derived from security testing was "used solely to promote the security of the owner or operator of [the] computer, computer system or computer network" or "shared directly with the developer of such computer, computer system, or computer network."[2117] Such criteria would appear to be of uncertain application to at least some of the activities proposed here. First, the security research sought would be aimed in part at advancing the state of knowledge in the field, and not "solely" aimed at promoting the security of the owner or operator of the computer, computer system, or computer network (assuming such an owner could be identified).[2118] Second, determining the relevant "developer" to whom information must be disclosed could be difficult if not impossible in some instances.[2119]

The Register therefore concludes that, based on the current record, the permanent exemptions embodied in sections 1201(j), 1201(f) and 1201(g) do not appear unambiguously to permit the full range of legitimate security research that could be encompassed by the proposed exemption.[2120] In light of this uncertainty, the Register proceeds to consider an exemption for the proposed uses. This corresponds to the Register's approach on the two earlier occasions when the Register concluded that section 1201's permanent exemptions were inadequate to facilitate important security research, and thus needed to be supplemented with exemptions adopted as part of the triennial rulemaking proceeding.[2121]

Finally, although, as opponents note, the 2006 and 2010 exemptions were aimed at analyzing security flaws in TPMs themselves, the Register does not see a legal or logical reason why the exemption cannot be aimed at the copyrighted computer programs

[2115] 17 U.S.C. § 1201(j)(1).

[2116] *See, e.g.*, Green Class 25 Supp. at 21-22.

[2117] 17 U.S.C. § 1201(j)(3)(A).

[2118] *See, e.g.*, Green Class 25 Supp. at 22

[2119] *See, e.g.*, *id.* at 21-22.

[2120] *See, e.g.*, *id.* at 19; *see also* CDT Supp. at 3-4; Green Class 25 Reply at 9; Tr. at 14:16-25, 17:13-19 (May 26, 2015) (Reid on behalf of Green).

[2121] 2006 Final Rule, 71 Fed. Reg. at 68,477 (granting an exemption for good-faith security research into sound recordings on compact discs); 2010 Final Rule, 75 Fed. Reg. at 43,832-33 (granting an exemption for good-faith security research on video games accessible on personal computers).

protected by a TPM. There is no such restriction contained in the language or legislative history of the DMCA, and section 1201(j) would arguably enable such research—albeit subject to the limitations of that section.

c. Statutory Factors

Turning to the statutory factors set forth in section 1201(a)(1), the Register finds that the first factor, concerning the availability for use of copyrighted works, slightly favors proponents.[2122] While proponents assert that allowing circumvention will permit greater "use" of the TPM-protected works at issue by virtue of the ability to circumvent, this would seem to prove too much, as presumably the same could be said of any requested exemption. The more salient consideration is whether there will be greater availability of copyrighted works in general if an exemption is granted. In this regard, the Register notes that opponents have not established that an exemption would have a negative impact on the availability of copyrighted works. On the other hand, proponents persuasively establish that an exemption could increase the availability of works based on security research, such as scholarly articles and presentations, as well as new computer programs aimed at rectifying discovered flaws.[2123] Therefore, this factor weighs somewhat in favor of the exemption.

Turning to the second factor, the availability for use of works for nonprofit archival, preservation and educational purposes,[2124] the Register finds that an exemption for good-faith security research is likely to increase the use of works in educational settings. The record indicates that the current prohibition plays a negative role in universities' willingness to engage in and fund security research, and may limit student involvement in academic research projects.[2125]

With respect to the third factor, proponents have established that the exemption will enhance criticism, comment, news reporting, teaching, scholarship and research. As noted with respect to the second factor, the record indicates that teaching and scholarship

[2122] 17 U.S.C. § 1201(a)(1)(C)(i).

[2123] *See, e.g.*, Bellovin et al. Supp. at 8; EFF Class 22 Supp. at 23 (citing to the scholarly papers and presentations that are created and published as a result of the ability to engage in good-faith security testing); MDRC Supp. at 11-13, 20 (stating the proposed exemption will facilitate the publication of articles based on findings of medical device software researchers).

[2124] 17 U.S.C. § 1201(a)(1)(C)(ii).

[2125] *See, e.g.*, Green Class 25 Supp. at 23; *see also* Bellovin et al. Supp. at 8 (contending that "information security education efforts are actively hampered [by the prohibition] on all levels of the educational system"); Tr. at 160:18-22 (May 26, 2015) (Bellovin) ("I cannot do grant-funded research that, with a contract, gives somebody else the right, precisely to preserve academic freedom and also to protect me and my students under the export laws."); Tr. at 75:05-76:12 (May 26, 2015) (Blaze); MDRC Supp. at 24 (noting that the use of medical device software for nonprofit educational purposes "is entirely unavailable for a device employing a TPM unless this exemption is granted").

would be enhanced by the proposed exemption.[2126] Additionally, the record establishes that research is at the core of the proposed exemption; adopting such an exemption would thus serve to promote research.[2127] Finally, the record suggests that the exemption could enhance media attention to, and reporting on, software security issues.[2128] Thus, this factor weighs strongly in favor of the exemption.

Regarding the fourth statutory factor,[2129] the Register determines that the effect of the exemption on the market for or value of copyrighted works would generally not be adverse. Although opponents assert that granting the exemption could erode the public's confidence in the safety and security of products that are found to be flawed, this is not a harm that the Register is comfortable crediting in this context. Such an adverse effect is not truly a copyright concern; it is more fairly traceable to the existence of security defects in computer programs rather than security researchers' access to those programs. Moreover, it can also be argued that knowledge of and ability to correct such flaws will in fact enhance the value of the software and products at issue. The Register thus finds this statutory factor to be neutral or, at most, to weigh marginally in favor of an exemption.

Finally, the statute also allows the Librarian to consider "such other factors" as may be appropriate.[2130] This "catchall" provision has played a significant role in the discussion and review of all the security research classes. To begin with, the Register notes that regulating disclosure of vulnerabilities may implicate First Amendment concerns. Proponents point to the Second Circuit's decision in *Universal City Studios, Inc. v. Corley*, which addressed some of the relevant constitutional principles, albeit in the context of a case arising under an anti-trafficking provision of section 1201 that rejected a First Amendment challenge to an injunction prohibiting disclosure of a decryption program.[2131] *Corley* explained that content-neutral speech regulations "must serve a substantial governmental interest, the interest must be unrelated to the suppression of free expression, and the incidental restriction on speech must not burden substantially more speech than is necessary to further that interest."[2132] GM, the only opponent in the instant proceeding to address the free speech issue, agrees that "any disclosure standard could raise First Amendment issues," although it suggests that "the protection afforded by the First Amendment to security vulnerabilities is limited."[2133] Although the Register

---

[2126] *See, e.g.*, Green Class 25 Supp. at 23; *see also* Bellovin et al. Supp. at 8; Tr. at 160:18-22 (May 26, 2015) (Bellovin); Tr. at 75:05-76:12 (May 26, 2015) (Blaze); MDRC Supp. at 24.

[2127] *See, e.g.*, EFF Class 22 Reply at 19; Schneier Class 22 Reply (offering that many security researchers refrain from conducting important security research because of fear of DMCA liability); EFF Class 22 Reply at 19; Green Class 22 Supp. at 1; EFF Class 22 Supp. at 23; MDRC Supp. at 24.

[2128] Bellovin et al. Supp. at 8; Bellovin et al. Reply at 11.

[2129] 17 U.S.C. § 1201(a)(1)(C)(iv).

[2130] *Id.* § 1201(a)(1)(C)(v).

[2131] 273 F.3d at 453-58.

[2132] *Id.* at 454.

[2133] GM Class 25 Post-Hearing Letter at 2.

does not opine on the extent to which First Amendment principles might cabin government efforts to adopt vulnerability disclosure standards, constitutional free speech principles are at least arguably relevant to any consideration of such standards here.

Opponents correctly observe that a security research exemption implicates significant health and safety considerations.[2134] These include automobile safety,[2135] environmental impacts,[2136] issues of patient health and privacy,[2137] personal security,[2138] and consumer reliance on the integrity of product design and operation.[2139] Opponents posit scenarios of bad actors invoking the exemption to do harm to persons or property, or to profit from their discoveries by threatening manufacturers with public disclosure in an irresponsible fashion.[2140] Opponents also point to the fact that many who make and market consumer products, including motor vehicles and medical devices, must comply with a host of federal and state regulatory mandates, and that the use of TPMs has played a role in ensuring such compliance.[2141] They further note that access to vehicle software could compromise safety- and emissions-based compliance regimes.[2142] These concerns cannot be easily dismissed. In light of the significant public policy issues that fall within the expertise and authority of other government agencies, and as suggested by some of the commenting parties, the Copyright Office advised the Department of Transportation ("DOT"), the Environmental Protection Agency ("EPA") and FDA of the pendency of

[2134] *See, e.g.*, AdvaMed Class 25 Opp'n at 22; Auto Alliance Class 25 Opp'n at 1 (citing Auto Alliance Class 22 Opp'n at 12-15) (asserting that there are "serious threats to safety and security that recognition of the proposed exemption would create or exacerbate"); GM Class 25 Opp'n at 18 (asserting that an exemption could make "it easier for both ill willed wrongdoers and unknowing hobbyists and the like to access a vehicle's software and compromise safety and regulatory compliance systems validated by the automaker").

[2135] *See, e.g.*, GM Class 25 Opp'n at 21.

[2136] *See, e.g.*, *id.* at 14; *see also* Tr. at 134:06-12 (May 26, 2015) (Lightsey, GM); GM Class 25 Post-Hearing Resp. at 2-3.

[2137] *See, e.g.*, AdvaMed Class 25 Opp'n at 5; *see also* LifeScience Alley Class 25 Opp'n at 4.

[2138] *See, e.g.*, AdvaMed Class 25 Opp'n at 2-3.

[2139] *See, e.g.*, *id.*; Auto Alliance Class 25 Opp'n at 1 (citing Auto Alliance Class 22 Opp'n at 12-15); GM Class 25 Opp'n at 18; LifeScience Alley Class 25 Opp'n at 4-6; MDISS Opp'n at 1; Tr. at 134:06-12 (May 26, 2015) (Lightsey, GM); Tr. at 132:20-21 (May 26, 2015) (Troncoso, BSA).

[2140] *See, e.g.*, Tr. at 125:11-17 (May 26, 2015) (Troncoso, BSA); *see also id.* at 135:10-16 (Lightsey, GM) (expressing concerns that "the ability for automobile manufacturers to control that research and to have the opportunity to fix vulnerabilities before they're widely disclosed would be severely limited and could thus create safety concerns"); GM Class 25 Opp'n at 6 (asserting that allowing circumvention "increases access to, and as noted by Proponents, *publication* of sensitive information relating to the operation of ECUs which in turn increases the risks to safety and security and other systems that an owner trusts"); BSA Post-Hearing Resp. at 1; GM Class 25 Post-Hearing Resp. at 2.

[2141] *See, e.g.*, AdvaMed Class 25 Opp'n at 2; GM Class 25 Opp'n at 14; IPO Class 25 Opp'n at 1; MDISS Opp'n at 1; Tr. at 134:06-12 (May 26, 2015) (Lightsey, GM).

[2142] GM Class 25 Opp'n at 17-18.

this proceeding, so that these agencies could provide input if they wished.[2143] The Office received letters from DOT, EPA, and FDA, all of which expressed significant reservations about the proposed exemptions.[2144] As discussed below, however, NTIA, which has an express statutory role in this rulemaking,[2145]supported adoption of a broad security research exemption.

In its letter addressing Proposed Class 22, DOT noted concerns over the nature and timing of the potential public disclosure of security research.[2146] While DOT recognized that enabling publication of good-faith research offers the potential benefit of promoting collaboration in identifying security vulnerabilities or other problems, it expressed concern that there could be circumstances in which security researchers might not fully appreciate the potential safety ramifications of their acts of circumvention or the logistical limitations associated with potential remedial actions.[2147] DOT also expressed that its concerns could be potentially addressed by appropriate limitations on disclosures of security research findings or by the provision of adequate time for responsive actions to be formulated and executed before broader disclosures are made.[2148]

In its communication, EPA urged the Office to decline to recommend the proposed exemption in Proposed Class 22 for vehicle software security research, expressing concern that granting this exemption "would enable actions that could slow or reverse gains under the Clean Air Act."[2149] In addition, EPA expressed concern that the

---

[2143] Letter from Jacqueline C. Charlesworth, Gen. Counsel and Assoc. Register of Copyrights, USCO, to Kathryn B. Thomson, Gen. Counsel, DOT, and Stephen P. Wood, Acting Chief Counsel, Nat'l Highway Traffic Safety Admin. (May 12, 2015); Letter from Jacqueline C. Charlesworth, Gen. Counsel and Assoc. Register of Copyrights, USCO, to Avi S. Garbow, Gen. Counsel, EPA (May 12, 2015); Letter from Jacqueline C. Charlesworth, Gen. Counsel and Assoc. Register of Copyrights, USCO, to Elizabeth H. Dickinson, Chief Counsel, FDA (May 12, 2015), *all available at* http://copyright.gov/1201/2015/USCO-letters.

[2144] Letter from Geoff Cooper, Assistant Gen., EPA, to Jacqueline C. Charlesworth, Gen. Counsel and Assoc. Register of Copyrights, USCO (July 17, 2015) ("EPA Letter"); Letter from Bakul Patel, Assoc. Dir. for Digital Health, Ctr. for Devices and Radiological Health, FDA, to Jacqueline C. Charlesworth, Gen. Counsel and Assoc. Register of Copyrights, USCO (Aug. 18, 2015) ("FDA Letter"); Letter from Kathryn B. Thomson, Gen. Counsel, DOT, to Jacqueline C. Charlesworth, Gen. Counsel and Assoc. Register of Copyrights, USCO (Sept. 9, 2015) ("DOT Letter"), *all available at* http://copyright.gov/1201/2015/USCO-letters. Consideration of these agency responses is appropriate because the matter of other agencies' potential concerns with respect to this exemption was raised by commenting parties and has been part of the record since the filing of opposition comments on March 27, 2015. *See, e.g.*, AdvaMed Class 25 Opp'n at 3. These concerns were also raised at the public hearings. *See, e.g.*, Tr. at 56:05-57:16 (May 19, 2015) (Charlesworth, USCO; Lightsey, GM). Proponents thus had the opportunity to address the concerns both in their reply comments and at the public hearings, and the record reflects significant public input on these issues in these classes.

[2145] 17 U.S.C. § 1201(a)(1)(C).

[2146] DOT Letter at 2-3.

[2147] *Id.*

[2148] *Id.*

[2149] EPA Letter at 1-2.

exemption would "hinder its ability to enforce the tampering prohibition" of the CAA. EPA explained that the agency "has taken enforcement action against third-party vendors who sell or install equipment that can 'bypass, defeat, or render inoperative' software designed to enable vehicles to comply with the [CAA] regulations."[2150] EPA therefore concluded that it "can curb this practice more effectively if circumventing TPMs remains prohibited under the DMCA."[2151]

FDA expressed concerns about the proposed exemptions in Class 27A, for medical device software security research, and in Class 25, for general software security research.[2152] FDA emphasized that, even if these exemptions are granted, FDA would retain regulatory jurisdiction over medical devices and the entities that manufacture those devices. At the same time, it noted that granting an exemption could "potentially create regulatory confusion for FDA, medical device manufacturers, and third party software developers that choose to modify medical devices."[2153] (Some of the concerns raised by FDA were more directly relevant to Proposed Class 27B, which is aimed at permitting patient access to information generated by the patient's device, and are further addressed below in that context.)

With respect to both Proposed Classes 25 and 27A, FDA expressed strong concern that the exemption, as proposed, "does not seem to make a distinction between bench top testing of device security and testing of a device in clinical use (i.e., an implant in an actual patient, a device in a hospital, etc.)."[2154] It emphasized that "[t]hese latter situations carry greater risk to patients and public health and may present challenges to FDA with respect to devices that have been manipulated."[2155] It thus "recommend[e]d that any final rule make a distinction between bench top testing of devices . . . and testing of devices during clinical use."[2156]

Moreover, FDA noted as a general matter that it had issued regulatory guidance in the area of security testing in which it recommended that "manufacturers consider cybersecurity risks as part of the design and development of a medical device, and submit

---

[2150] *Id.* at 3.

[2151] *Id.* The Register further notes that to the extent EPA or another federal or state agency itself seeks to investigate—or appoint agents to investigate—alleged violations of the law, that agency should be able to rely on the permanent exception set forth in section 1201(e) for law enforcement activities, which allows "lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State." 17 U.S.C. § 1201(e).

[2152] FDA Letter at 1.

[2153] *Id.*

[2154] Bench top testing refers to testing "where the unit tested is not in clinical use and will not be in clinical use in the future." *Id.* at 4.

[2155] *Id.*

[2156] *Id.* at 4, 5.

documentation to the FDA about the risks identified and controls in place to mitigate those risks."[2157] While acknowledging that "there could be risks and benefits of enabling 'good-faith' research for the purpose of identifying, disclosing, and fixing malfunctions, security flaws, or vulnerabilities," FDA explained that "a risk to opening technology in this way is the difficulty for regulators and others to distinguish 'good-faith' research efforts from malevolent third-party actors." In addition, FDA expressed worry that "this exemption may cause confusion for stakeholders that have been advised through FDA guidance to put appropriate cybersecurity controls in place to prevent third parties from manipulating the software of the device."[2158]

On this record, the Register is persuaded that, under the fifth statutory factor allowing for consideration of additional matters as appropriate, the significant issues raised by opponents concerning public safety and regulatory compliance, as amplified by regulatory agencies with a direct interest in these matters, are unfavorable to the proposed exemption. Despite the fact that the other statutory factors largely favor proponents, the Register must take seriously these additional substantial concerns.

4. NTIA Comments

Like the Register, NTIA concludes that "good faith security researchers and academics are currently being deterred from engaging in noninfringing activities due to the threat of litigation under section 1201,"[2159] and that the permanent exemptions in sections 1201(f), 1201(g), and 1201(j) are "not sufficient to obviate the need for a broad good faith security exemption."[2160] NTIA accordingly supports a broad security research exemption in Class 25 for all "computer programs . . . regardless of the device on which they are run."[2161] NTIA explains that this exemption would also "serve to exempt the security research activities contemplated in Classes 22 and 27 (directed at vehicles and networked medical devices, respectively)."[2162] NTIA also recommends that the exemption state explicitly that it "does not obviate the need to comply with other applicable laws and regulations,"[2163] in recognition of the fact that "an exemption would not preclude liability under laws such as the CFAA."[2164] And, as discussed above in Class 21, NTIA acknowledges that, in light of the safety and security concerns that might be implicated by the exemption, the Register might find it appropriate to "delay the date upon which . . . an exemption would become effective to allow the relevant stakeholders

[2157] *Id.* at 4.

[2158] *Id.*

[2159] NTIA Letter at 72.

[2160] *Id.* at 76.

[2161] *Id.* at 89.

[2162] *Id.* at 88.

[2163] *Id.* at 89.

[2164] *Id.* at 72.

in other policy spheres to prepare for the exemption's effective date."[2165] NTIA stresses, however, that any such delay should be "as short as practicable."[2166]

As explained below, the Register agrees with NTIA that the Librarian should grant the exemptions for good-faith security research in Proposed Classes 25, 22 and 27A, although with certain limitations based on the rulemaking record. The Register also recommends that other interested agencies be afforded a window of time to prepare for the new rule.

5. Conclusion and Recommendation

The policy concerns reflected in the three security research proposals represented by Proposed Classes 25, 22, and 27A, and in the forceful responses thereto, are substantial ones that are more properly debated in the halls of Congress—or at least the halls of other federal agencies. Especially in light of near-daily reports of major security breaches in both government and private-sector computer systems, the importance of good-faith security research to identify and address software flaws and malfunctions probably cannot be overstated. At the same time, it is apparent that there is much to be weighed in determining the best path forward.

The rules that should govern such research hardly seem the province of copyright, since the considerations of how safely to encourage such investigation are fairly far afield from copyright's core purpose of promoting the creation and dissemination of creative works. Rather, the rules that should govern are best considered by those responsible for our national security and for regulating the consumer products and services at issue. That said, it is inescapable that the anticircumvention prohibition in section 1201(a)(1) plays a role in the debate. Indeed, Congress recognized as much in enacting section 1201 when it included a standing exemption for security testing in section 1201(j). But while Congress clearly foresaw the need to facilitate good-faith security research, it is less clear that the exemption has been as effective as it needs to be. Proponents of the security-related exemptions have put forth a convincing case in this proceeding that section 1201(j) does not provide enough certainty to ensure that certain types of legitimate research are able to move forward.[2167]

Significantly, the views within the Administration itself appear to be sharply divided on the issues surrounding security research and the wisdom of granting an exemption for this purpose, with NTIA favoring a broad exemption, EPA opposing an exemption, and DOT and FDA expressing notable reservations. Given the disagreement

[2165] *Id.* at 5.

[2166] *Id.*

[2167] *The Register's Perspective on Copyright Review: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 28-30 (2015) (statement of Maria A. Pallante, Register of Copyrights and Dir., USCO) (The Register observed the limited nature of the security testing exemption in section 1201(j) and supported congressional review of the problem.).

among these other agencies, the Register recommends that the Librarian exercise a degree of caution in adopting an exemption.

After consideration of the entire record, and as described in more detail below, the Register concludes that the Librarian would be best advised to adopt an exemption that, while building upon Congress's intent in section 1201(j), will also serve to mitigate certain statutory constraints on the conduct of good-faith security research. This exemption should encompass the types of software that were the focus of the record in this proceeding, namely computer programs contained in devices and machines primarily designed for use by individual consumers, motorized land vehicles, implanted medical devices and their corresponding home monitoring systems, and voting machines. The record does not support the open-ended exemption urged by Class 25 proponents, encompassing all computer programs on all systems and devices, including highly sensitive systems such as nuclear power plants and air traffic control systems. As Congress made clear in enacting section 1201, the "'particular class of copyrighted works' [is intended to] be a *narrow and focused subset* of the broad categories of works . . . identified in section 102 of the Copyright Act."[2168] Accordingly, as in past rulemakings, the Register must craft an exemption based on the evidentiary showing of adverse effects.[2169] Here, as discussed above, proponents' arguments in Class 25 focused largely on consumer-oriented software and products. No showing was made to justify access to other types of software or systems or explain how such an exemption would work. Accordingly, the exemption is limited in that respect.[2170]

The recommended exemption accounts for several other concerns as well. First, the exemption must allow some room for other interested agencies to weigh in on this national debate. Opponents and other federal agencies have raised serious public health and safety concerns regarding the acts of circumvention being proposed. Even as limited by the Register, the recommended exemption is broad enough to cover any number of highly regulated products. Accordingly, to give other parts of the government an opportunity to respond, as a general matter the exemption should not go into effect until twelve months after the effective date of the new regulation.[2171] The Register concludes

[2168] H.R. REP. NO. 105-551, pt. 2, at 38 (1998) (emphasis added).

[2169] *See, e.g.*, 2010 Recommendation at 16 (explaining that "[t]he records in [the 2010] and prior rulemaking proceedings have demonstrated that in many cases, [an initial] subset of a category of works should be further tailored in accordance with the evidence in the record").

[2170] Proponents raised the possibility that certain software may be used both on consumer devices and on industrial ones. *See* Tr. at 114:11-115:05 (May 26, 2015) (Stallman, CDT; Damle, USCO) ("[M]any of those systems that we think of as critical infrastructure oftentimes depend on the same type of security that's running applications and services that we think of as noncritical infrastructure."). In that circumstance, security research into such software would be permitted where it is conducted on a consumer device, but not when it is conducted on an industrial one.

[2171] The Register understands the Librarian to have the discretion to phase in an exemption as required to address concerns in the record. Section 1201 allows the Librarian to deny exemptions outright, including based on the assessment of "such other factors as [he] considers appropriate" under the fifth statutory factor of section 1201(a)(1). *See* 17 U.S.C. § 1201(a)(1). Thus, the Librarian has the discretion to deny the

however, that such a delay is not warranted with respect to voting machines, as there is no record of public safety concerns with respect to these devices. Accordingly, especially in light of the upcoming presidential election, in the case of voting machines, the Register recommends immediate implementation.

Second, in light of the concerns raised by opponents, as well as DOT, EPA, and FDA, about the potential for any exemption to undermine other legal or regulatory mandates, any actions taken under the exemption will need to be compliant with all applicable laws and regulations. Accordingly, the Register recommends, consistent with the congressionally enacted exemption in section 1201(j), that the exemption require explicitly that the covered security research be lawful, including with respect to the CFAA.

Third, the Register takes seriously the concern expressed by other agencies that acts of security testing not put members of the public at risk. On this record, there appeared to be some consensus as to common-sense limitations on the exemption to avoid that risk. In the context of a general security research exemption, there appeared to be universal agreement among proponents that testing in "live" conditions—such as cars being driven on public roads—is wholly inappropriate.[2172] The Register thus recommends that the exemption provide that security research must be conducted in a controlled setting designed to avoid harm to individuals or the public. FDA also expressed specific concern about security testing of medical devices that are being used, or could be used, by patients, and recommended generally excluding such testing from the exemption.[2173] The Register agrees, and consequently recommends that the exemption for medical devices be specifically limited to devices that are not and will not be used by or for patients.

Fourth, as discussed above, a significant point of contention involves the proper disclosure of security research findings. It is apparent that the interests of the manufacturer and the public may both be affected by the nature and timing of disclosure of software flaws.[2174] Indeed, Congress included disclosure to the developer as one of the factors to be considered in determining a person's eligibility for the security testing exemption in section 1201(j).[2175] The Register similarly favors responsible disclosure of security flaws. But the Register also appreciates that appropriate disclosure standards are

---

proposed exemption at issue here, based on the substantial safety and environmental concerns presented in the record, with the understanding that it could be reconsidered in the next triennial proceeding. The Register, however, does not find outright denial to be necessary in this case. The Register understands the power to deny an exemption to carry with it the ability to designate a period of time before it becomes effective in lieu of denying the exemption entirely in order to address legitimate concerns in the record.

[2172] *See, e.g.*, Tr. at 150:16-20 (May 26, 2015) (Blaze); *id.* at 139:03-08, 141:15-20, 23-25 (Green); *id.* at 144:02-06 (Reid on behalf of Green).

[2173] FDA Letter at 5.

[2174] *See, e.g.*, GM Class 25 Post-Hearing Resp. at 2.

[2175] 17 U.S.C. § 1201(j)(3).

a divisive topic among security researchers and for the affected industries. Furthermore, the Register acknowledges that definitive disclosure requirements might implicate First Amendment concerns. In this arena, copyright law does not provide an answer; rather, other legal regimes, regulatory authority and industry norms should come to bear. Accordingly, rather than attempt to break new ground regarding disclosure requirements, the Register recommends that the exemption simply reflect what the Register understands to be the basic intent of section 1201(j), by specifying that the research activities and information derived therefrom primarily promote the security of the types of devices containing the computer programs on which the research is conducted, or those who use those devices. Bad-faith activities, including irresponsible disclosure, would thus cause the research to fall outside of the exemption.

Finally, the Register notes that in the interest of adhering to Congress's basic purpose in section 1201(j), where appropriate, the recommended exemption tracks Congress's language rather than the alternative formulations suggested by proponents.

Accordingly, the Register recommends that the Librarian designate the following class:

(i) Computer programs, where the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates solely for the purpose of good-faith security research and does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986, as amended and codified in title 18, United States Code; and provided, however, that, except as to voting machines, such circumvention is initiated no earlier than 12 months after the effective date of this regulation, and the device or machine is one of the following:

(A) A device or machine primarily designed for use by individual consumers (including voting machines);

(B) A motorized land vehicle; or

(C) A medical device designed for whole or partial implantation in patients or a corresponding personal monitoring system, that is not and will not be used by patients or for patient care.

(ii) For purposes of this exemption, "good-faith security research" means accessing a computer program solely for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability, where such activity is carried out in a controlled environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of

devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement.

K. Proposed Class 23: Abandoned Software – Video Games Requiring Server Communication

1. Proposal

Many modern video games—which may be played on a personal computer ("PC") or a dedicated gaming console—require a network connection to a remote server operated by the game's developer to enable core functionalities, such as gameplay. First, before some games can be played at all, including in single-player mode, the game must connect to an "authentication server" to verify that the game is a legitimate copy. This connection or "check" may be made once, at initial installation, or periodically throughout gameplay. Second, some games require a connection to a "matchmaking server" to enable users to play the game with other people over the internet in multiplayer mode. A matchmaking server connects computers at remote locations together to play a game at the same time, and may also allow access to "downloadable content, leaderboards, badges, chat, and other social features."[2176] In the case of a game that relies on an authentication server, the game may be rendered entirely unplayable if the server connection is lost. In the case of a matchmaking server, only multiplayer play over the internet would be disabled; in most cases, the game would still be playable in single-player mode, or with multiple players through a local area network connection.

Proposed Class 23 would allow circumvention of access controls on video games that require communication with a server to allow for continued gameplay or multiplayer play over the internet after the game's developer (or publisher or authorized service provider) has ceased supporting server communications for the game.[2177] The Electronic Frontier Foundation ("EFF") and Kendra Albert, a student at Harvard Law School, jointly filed a petition seeking an exemption to enable those who have lawfully acquired copies of video games to gain access to games when authentication or matchmaking servers have been permanently taken offline.[2178] The NPRM described the class as follows:

> Proposed Class 23: This proposed class would allow circumvention of TPMs on lawfully acquired video games consisting of communication with a developer-operated server for the purpose of either authentication or to enable multiplayer matchmaking, where developer support for those

[2176] The Entertainment Software Association ("ESA") Class 23 Opp'n at 8.

[2177] *See generally* the Electronic Frontier Foundation & Kendra Albert ("EFF/Albert") Class 23 Supp. at 2-5. Opponents object to referring to this class as "abandoned" software, noting that the copyright owners have not "abandoned" their rights in the software. ESA Class 23 Opp'n at 5. To clarify, the Register's use of "abandonment" in this context refers only to withdrawal of support for servers that are necessary for certain aspects of gameplay, not any rights related to the video game.

[2178] EFF/Albert's proposed regulatory language reads as follows: "Literary works in the form of computer programs, where circumvention is undertaken for the purpose of restoring access to single-player or multiplayer video gaming on consoles, personal computers or personal handheld gaming devices when the developer and its agents have ceased to support such gaming." EFF/Albert Pet. at 1; *see also* EFF/Albert Supp. at 1.

> server communications has ended. This exception would not apply to video games whose audiovisual content is primarily stored on the developer's server, such as massive multiplayer online role-playing games.[2179]

In addition to EFF/Albert, comments supporting the proposed exemption were filed by Free Software Foundation ("FSF"), eBay, Inc. ("eBay"), the Preservation and Reformatting Section of the Association for Library Collections and Technical Services ("PARS"), Catherine Gellis and the Digital Age Defense project ("Gellis/Digital Age Defense"),[2180] and over 1230 individuals.[2181]

The EFF/Albert proposal focused in particular on two specific users and uses: (1) people who wish to continue to play physical or downloaded copies of video games they have lawfully acquired (referred to herein as "gamers"); and (2) libraries, archives and museums that seek to preserve individual video games and make them available for research and study (referred to as "preservationists").[2182] In terms of making video games available for research and study, proponents seem mainly to contemplate playable games in an archival or exhibition setting, rather than distribution to or off-site access by members of the public.[2183] The proposal describes the scope of the exemption as extending to video games that "run on personal computers, game consoles, or handheld gaming devices."[2184] Even though the proposal references only the video games

[2179] NPRM, 79 Fed. Reg. at 73,869.

[2180] Gellis/Digital Age Defense Class 23 Supp.

[2181] EFF/Albert Supp.; FSF Class 23 Supp.; eBay Class 23 Reply; PARS Reply; Digital Right to Repair Class 23 Supp. (1145 individuals); Digital Right to Repair Class 23 Reply (74 individuals); Mike Battilana Class 23 Supp.; Christian Clark Class 23 Reply; Juan Pablo Zapata Díaz Class 23 Reply; Fatih Gencer Class 23 Reply; Robert Heltzel Reply; Michael Horton Class 23 Reply; Philip John Reply; David Labovitch Reply; James O'Neill Reply; Alex Santa Maria Reply; Anthony Valunas Reply.

[2182] EFF/Albert Pet. at 2; *see also* EFF/Albert Supp. at 8; Tr. at 197:25-198:06 (May 20, 2015) (Stoltz, EFF) (asserting that "the goal of preservation is to preserve every aspect of the original experience of playing a game, to provide really the maximum amount of data and experiential data for the future, whether that is a museum exhibit for academics or whatever use coming down the road"). PARS also seeks to include educational institutions in the exemption, but does not provide any basis for including them. *See* PARS Reply at 2.

[2183] *See, e.g.*, EFF/Albert Supp. at 8 & n.52 (citing Paola Antonelli, Video Games: 12 in the Collection, for Starters, MOMA INSIDE/OUT (Nov. 29, 2012) http://www.moma.org/explore/inside_out/2012/11/29/video-games-14-in-the-collection-for-starters ("Antonelli")); *id.* at 8 & n.53 (citing *Video and Other Electronic Game Collections*, THE STRONG: NATIONAL MUSEUM OF PLAY, http://www.museumofplay.org/collections/video-and-other-electronic-game-collections (last visited Oct. 7, 2015) ("*Video and Other Electronic Game Collections*")); *id.* at 8 & n.54 (citing *About Us*, THE MUSEUM OF ART AND DIGITAL ENTERTAINMENT: OAKLAND'S VIDEOGAME MUSEUM, http://themade.org/what-are-we (last visited Oct. 7, 2015) ("MUSEUM OF ART AND DIGITAL ENTERTAINMENT: ABOUT US")); PARS Reply at 2.

[2184] EFF/Albert Pet. at 2; *see also* EFF/Albert Supp. at 2. While proponents provide specific evidence related to console-based and PC video games, they provide little to no evidence on handheld games. *See* EFF/Albert Supp. at 6 (arguing that "[c]onsole games are often hit the hardest by server shutdowns," but

themselves, as the record developed, it became clear that the exemption might to some extent also implicate jailbreaking of video game consoles, a matter which is further discussed below.

EFF/Albert limit the proposed exemption to "lawfully acquired" video games,[2185] alternately described as games that users "lawfully own"[2186] or have "purchased."[2187] From proponents' descriptions of the activities they wish to undertake, it appears that proponents are referring to users who lawfully possess a physical or downloaded copy of a game, and not merely the right to access or play a game through a subscription or by other means.[2188]

EFF/Albert further qualify the requested exemption in two significant ways. First, they exclude from the request video games that feature "persistent worlds," or games where a user accesses "a hosted world that remains static and intact when players have signed off."[2189] For example, the proposed exemption would exclude massively multiplayer online roleplaying games such as World of Warcraft or EVE Online.[2190] EFF/Albert explain that these "[p]ersistent worlds require 'robust servers designed to host hundreds, if not thousands of simultaneous players,' and cannot generally be re-created after a shutdown without the cooperation of the game's developer."[2191]

Second, EFF/Albert propose that for purposes of the proposed exemption, the condition that developer support for an authentication or matchmaking server has ended can be met in one of two ways: either the developer affirmatively announces that the game is no longer supported, or the gameplay or multiplayer server is not accessible by players for at least six months.[2192]

---

also that "much of the activity surrounding restoration of play for abandoned games has occurred for PC games").

[2185] EFF/Albert Supp. at 1.

[2186] *Id.* at 8.

[2187] *Id.* at 2.

[2188] *See, e.g.*, EFF/Albert Reply at 4 (stating that the exemption is limited to "[l]awful [p]ossessors" of games); EFF/Albert Supp. at App. (Statement of Alex Handy and Statement of John Doe); eBay Class 23 Reply at 2.

[2189] EFF/Albert Supp. at 2, App. (Statement of Alex Handy).

[2190] *Id.*

[2191] *Id.* Acknowledging opponents' concern that some persistent world games store copyrighted content locally, EFF/Albert ultimately proposed that "persistent world games" be defined as those that "can[not] be restored after server shutdown *without* making new, permanent copies of any original audiovisual content." EFF/Albert Reply at 4.

[2192] EFF/Albert Supp. at 3. In cases where such games are subsequently re-released, EFF/Albert contend that the publisher or new rightsholder is likely to restore functionality through the application of new or updated access controls, and concede that the exemption would not allow circumvention of these access controls. *Id.*

a. Background

According to proponents, requiring that a video game communicate with a third-party server before enabling play, as well as the specific server protocols or cryptographic verification used in that process, can constitute TPMs subject to section 1201's prohibition on circumvention.[2193] Proponents describe several methods of circumventing these TPMs. For authentication servers, they explain that video game software can be modified to remove the requirement that the game check in with the authentication server as a condition for gameplay.[2194] Alternatively, the authentication server can be emulated by reverse engineering the communications that the game expects to receive from the server.[2195]

For matchmaking servers, proponents assert that circumvention generally involves establishing a replacement matchmaking server and coordinating with users who wish to continue multiplayer play so that they can modify copies of the game software to allow them to connect to the replacement server.[2196] Enabling multiplayer play once the game developer has terminated server support may also require replicating or creating new protocols to communicate with the game, and distributing the new protocols (including a new IP address) to gamers at different locations.[2197] EFF/Albert concede that modification of game software for such purposes may result in the creation of "a derivative work, in the form of a new version of the game that will play without a server authentication check or one that connects to new matchmaking servers."[2198]

As explained below, opponents argue that proponents understate the nature of the TPMs at issue because enabling continued play for many games would "require circumvention of a much broader array of video game and device-based access controls" that could include "jailbreaking" of video game consoles.[2199] EFF/Albert respond,

---

[2193] *Id.* at 4 (specifically referencing SSL certificates and age-checking).

[2194] *Id.* at 1-2; Battilana Supp. at 3.

[2195] Battilana Supp. at 3; EFF/Albert Pet. at 4.

[2196] EFF/Albert Supp. at 4-5. As described by EFF, circumvention to engage in multiplayer play "involves watching network packets as they travel over the network, essentially testing a simulated server communication with one copy of the game and to see to what signals the game responds to and then writing and as an original work a server that can generate those communications. And those communications at the simplest are going to be 'you are allowed to run' and at the more complex level, they are 'Kendra and Cathy are online right now and would like to play, here are the messages that will initiate your playing against each other.'" Tr. at 200:16-201:02 (May 20, 2015) (Stoltz, EFF).

[2197] *See* EFF/Albert Supp. at 4-6; Mr.Game20, *Toorcon: San Diego (2014) – Cyber Necromancy: Reverse Engineering Dead Protocols*, YOUTUBE (Oct. 30, 2014), https://www.youtube.com/watch?v=K4dyyLpMkQk (cited in EFF/Albert Supp. at 4 n.18); Tr. at 201:17-202:06 (May 20, 2015) (Albert) (describing various circumvention methods to continue multiplayer gaming, including changing a game's IP address so that gamers can connect to a new server).

[2198] EFF/Albert Supp. at 6.

[2199] ESA Class 23 Opp'n at 8; *see also id.* at 3 ("[T]here is no such thing as specific access controls that check 'authentication servers' and 'matchmaking servers' for video games . . . . Many of these access

however, that these broader access controls are specific to "modern consoles," and do not apply to PC-based games or older consoles.[2200] According to EFF/Albert, on older consoles, the TPMs for authentication and matchmaking operate separately from other TPMs that control gameplay, meaning that the modifications that would be required to restore the game to functionality under the proposed exemption "[would] not permit the playing of unauthorized copies of games."[2201] For newer consoles, EFF/Albert acknowledge that jailbreaking the console could be required to continue playing certain games, depending upon how a particular game is coded.[2202]

At the hearing, proponents indicated that the exemption they are seeking does not need to include jailbreaking of consoles by gamers.[2203] For preservation uses, however, EFF asserts that console jailbreaking should be part of the exemption.[2204] While it is not entirely clear why proponents draw a distinction between the needs of gamers and preservationists in this regard, as discussed below, the distinction is significant in evaluating the proposed exemption.

b. Asserted Noninfringing Uses

The Register notes that at the public hearing for this class, several witnesses delivered impassioned and moving explanations of the cultural, historical and educational significance of video games.[2205] These witnesses testified in particular to the personal and social loss when such games are taken off the market and are no longer available for play. EFF/Albert urge that the continued ability to play games that are no longer supported, as well as preservation and exhibition of those games, constitute noninfringing

---

controls serve a protective function that is far broader than 'authentication' or 'matchmaking.'"). "Jailbreaking" describes the process by which a console owner circumvents the TPMs on a video game console in order to install a different operating system or run software and games that are not vendor-approved. *See* 2012 Recommendation at 26.

[2200] EFF/Albert Reply at 5-6.

[2201] *Id.* at 5.

[2202] Tr. at 173:22-174:03 (May 20, 2015) (Damle, USCO; Albert) (identifying a game on a newer console that would require jailbreaking the console for continued play); *id.* at 202:25-203:08 (Albert) (asserting that older consoles do not require jailbreaking for continued play, but noting that newer generation consoles may require jailbreaking, "depend[ing] on how the game is coded").

[2203] *Id.* at 203:11-204:03 (Damle, USCO; Charlesworth, USCO; Albert) ("MR. DAMLE: If hypothetically we were to say you could make changes to the game, you could set up your own server but you can't touch the console, would that basically solve your concerns? You can't jailbreak a console. MS. ALBERT: Yes, jailbreaking a console is a different case. MS. CHARLESWORTH: So just to be clear, you think there is a solution that would solve your problem that would not require us to allow jailbreaking of consoles. MS. ALBERT: Yes . . . . I think that there are many games in which you can change the multiplayer or change the authentication without jailbreaking the console . . . . [J]ailbreaking the console is a separate 1201 issue.").

[2204] *Id.* at 254:25-255:03 (Stoltz, EFF) ("I want to emphasize that we are asking for an exemption that would cover the preservation of games on consoles that would . . . require in some sense jailbreaking.").

[2205] *See, e.g.*, *id.* at 164:10-165:21 (Diamante, Museum of Art and Digital Entertainment); *id.* at 175:08-176:08 (Albert); *id.* at 180:25-184:04 (Gholami, Azentium).

fair uses under section 107, and that each of the four fair use factors supports this view.[2206] Proponents assert no basis other than fair use to establish that the activities in question are noninfringing.

On the first fair use factor, EFF/Albert contend that the purpose and character of the use weighs in favor of a finding of fair use because enabling lawful copies of the game to interoperate with new servers is "a favored purpose under copyright law" and because "modifying a lawful, personal copy is noncommercial."[2207] In their analysis, EFF/Albert rely upon two Ninth Circuit cases, *Sega Enterprises Ltd. v. Accolade, Inc.*[2208] and *Sony Computer Entertainment, Inc. v. Connectix Corporation*,[2209] noting that both cases held that reverse engineering of video games for the purpose of determining the requirements for interoperability is a noninfringing fair use.[2210]

Second, EFF/Albert argue that the nature of the copyrighted work also weighs in favor of fair use because "[m]odifying a game to re-enable its functionality using a new server, or by disabling a server requirement, involves changing only functional aspects of the software, not expressive elements such as graphics or audio."[2211] Moreover, EFF/Albert assert that "[p]urely functional software code intended to inhibit interoperability carries only a thin copyright interest, which is overcome by the need to modify it to achieve interoperability."[2212]

Third, regarding the amount and substantiality of the work used, EFF/Albert concede that the amount of video game code that is used "may vary;" nonetheless, they assert that any copying and modification required to restore functionality is "the minimum needed in order to allow the game to be playable" and "a very small portion of the overall software."[2213] They therefore maintain that this factor supports a finding of fair use.

Fourth, EFF/Albert assert that the fourth factor, the effect on the market for or value of the copyrighted work, also weighs in favor of fair use because "[c]ircumventing server authentication or running new multiplayer servers does not harm the market for an abandoned game and may in fact increase its value to forward-looking consumers who

---

[2206] EFF/Albert Supp. at 6-8. The factors to be considered in a fair use analysis include: "(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work." *See* 17 U.S.C. § 107.

[2207] EFF/Albert Supp. at 7.

[2208] 977 F.2d 1510 (9th Cir. 1992).

[2209] 203 F.3d 596 (9th Cir. 2000).

[2210] EFF/Albert Supp. at 7.

[2211] *Id.*

[2212] *Id.*

[2213] *Id.*

value the long-term playability of a game."[2214] Further, they acknowledge that while some modern games require jailbreaking of consoles in order to connect to a remote server, games played on older consoles do not, and that consequently allowing circumvention for these games on older consoles would not trigger opponents' concerns over jailbreaking.[2215]

c. Asserted Adverse Effects

EFF/Albert claim that both gamers and preservationists are adversely affected by the prohibition on the circumvention of TPMs restricting use of video games for which developers have ended server support. EFF/Albert urge that video games are a "vital part of American cultural heritage and creativity"[2216] and that when authentication or matchmaking servers are shut down, the effects are severe both for gaming communities, who lose access to works that may hold significant meaning for them, as well as preservationists, who are thwarted in their efforts to preserve video games and make them available for study.[2217]

EFF/Albert explain that gamers' interest in an exemption is "to be able to continue to play games they have lawfully purchased."[2218] They also claim that "absent circumvention to restore access, server shutdowns degrade or destroy the value of a consumer's investment in a game."[2219]

With respect to preservationists, EFF/Albert assert that section 1201(a)(1) deters efforts at archiving and preserving video games, which in turn impedes research efforts into the medium. In their view, "[v]ideo games are cultural artifacts worthy of study."[2220] They explain that "[s]tudying older games creates a critical discourse and literature, [which are] key to understanding the current medium."[2221]

EFF/Albert provide statements of video game preservationists and scholars highlighting the need to preserve video games for future research and study.[2222] In

---

[2214] *Id.* at 7-8.

[2215] Tr. at 173:22-24 (May 20, 2015) (Albert).

[2216] EFF/Albert Supp. at 8 (citing Joseph Bernstein, *Meet the Men Trying To Immortalize Video Games*, BUZZFEED NEWS (Oct. 27, 2014), http://www.buzzfeed.com/josephbernstein/meet-the-men-trying-to-immortalize-video-games#.akGjX0xAj).

[2217] *See* Tr. at 175:08-176:04 (May 20, 2015) (Albert).

[2218] EFF/Albert Supp. at 10.

[2219] EFF/Albert Reply. at 12.

[2220] EFF/Albert Supp. at 9.

[2221] *Id.*

[2222] *Id.* at App. (Statement of Jason Scott, Internet Archive) ("The Internet Archive is interested in continuing to digitize and make available games to the public. However, as we come up to more current operating systems, and more modern examples, authentication servers start becoming part of the picture . . . . In order to continue to preserve and archive these games as they start to rely on authentication servers, we will need to deactivate the server authentication mechanism."); *id.* at App. (Statement of T.L. Taylor,

particular, EFF/Albert cite a report of the Preserving Virtual Worlds project, sponsored in part by the Library of Congress, which states that "the Digital Millennium Copyright Act's prohibition on defeating technological protection measures makes it impossible for a library to create a preservation copy of games employing DRM [digital rights management] and anti-copying measures."[2223] In some cases, preservationists may see a need to circumvent video game console software in order to enable a console-based game to be playable and thus accessible.[2224] EFF/Albert add that "players and amateur collectors" can aid in preservation efforts, performing "a significant amount of the legwork involved in saving [the games]."[2225] EFF/Albert also assert that adverse impacts are likely to increase as video games increasingly employ online DRM technologies.[2226]

Further, proponents reject various alternatives to circumvention, concluding that they are not "viable," "feasible" or "effective."[2227] Offering an example where licensing costs were allegedly prohibitive,[2228] EFF/Albert assert that obtaining a license from copyright owners is "not feasible for informal player communities who simply want to continue playing games they already own."[2229] On the other hand, Albert concedes that, in some cases, users "would gladly pay huge amounts of money to be able to play these games online again."[2230] Albert also asserts that licensing is not a realistic option because "finding all rightsholders can be difficult or impossible" due to a growing number of orphan works in the video game industry.[2231] EFF/Albert believe that even if licensing

---

Massachusetts Institute of Technology) ("The ability to explore old games, including seeing how a multiplayer function actually worked, is an incredibly valuable pedagogical tool.").

[2223] *Id.* at 13 (quoting JEROME MCDONOUGH, ET AL., PRESERVING VIRTUAL WORLDS FINAL REPORT 6 (2010), *available at* https://www.ideals.illinois.edu/handle/2142/17097 ("PRESERVING VIRTUAL WORLDS REPORT")). The Preserving Virtual Worlds project was a research venture of four universities and Linden Lab, supported by the Library of Congress's National Digital Information Infrastructure for Preservation Program, investigating issues concerning the preservation of video games and interactive fiction through a series of case studies. PRESERVING VIRTUAL WORLDS REPORT at 5.

[2224] Tr. at 255:01-03 (May 20, 2015) (Stoltz, EFF).

[2225] EFF/Albert Supp. at 9.

[2226] *Id.* at 10-11; EFF/Albert Reply at 9.

[2227] EFF/Albert Supp. at 12.

[2228] Tr. at 260:17-261:05 (May 20, 2015) (Charlesworth, USCO; Albert) (Albert stating that she is aware of an example of "someone who approached a video game company and couldn't afford a license," but explaining that she cannot provide details "because they asked me not to say who it was because they were concerned about the confidentiality of the information").

[2229] EFF/Albert Supp. at 12; *see also* Tr. at 259:12-260:04 (Albert) (stating that "prohibitive amounts of money" are required to "go through the licensing route").

[2230] Tr. at 175:15-17 (May 20, 2015) (Albert).

[2231] EFF/Albert Supp. at 12. An ''orphan work'' is an original work of authorship for which a good-faith, prospective user cannot readily identify and/or locate the copyright owner in a situation where permission from the copyright owner is necessary as a matter of law. U.S. COPYRIGHT OFFICE, REPORT ON ORPHAN WORKS 1 (2006), *available at* http://www.copyright.gov/orphan/orphan-report.pdf.

were feasible, it "cannot be considered an alternative to an exercise of fair use," which "does *not* require permission from the rightsholder."[2232]

EFF/Albert also reject the use of video-capture technology to memorialize video games by recording gameplay footage and "other non-play alternatives," contending that they "do[] not replicate the experience of actually playing the game, and [are] of much less value to scholars, not to mention to players who have lawfully purchased a game and wish to continue to play."[2233]

d. Argument Under Statutory Factors

While EFF/Albert contend that the statutory factors set forth in section 1201(a)(1) support an exemption for both gamers and preservationists, they emphasize in particular that preservation "is exactly the type of behavior that this exemption process is meant to protect."[2234]

With respect to the first factor, concerning the availability for use of copyrighted works, EFF/Albert assert that by definition "server shutdowns . . . have a significant impact on the availability for use of many games."[2235]

As for the second statutory factor, regarding nonprofit archival, preservation, and educational purposes, EFF/Albert urge that these purposes will be hindered without an exemption. EFF/Albert claim that "[r]emoval of authentication mechanisms and restoration of multiplayer functionality to legally purchased games . . . assists the archiving and preservation of cultural works."[2236] Here again, EFF/Albert rely on the Preserving Virtual Worlds report and its opinion that the DMCA's prohibition on circumvention prevents libraries from creating preservation copies "of games employing DRM and anti-copying measures."[2237]

Considering the third factor, which addresses the impact of the prohibition on criticism, comment, news reporting, teaching, scholarship, and research, EFF/Albert claim that scholars and teachers must "access older works" and "replicate the experience of originally playing the game" to teach game design or theories behind game construction.[2238]

For the fourth factor, the effect of circumvention on the market for or value of copyrighted works, EFF/Albert argue that an exemption would not harm the market

---

[2232] EFF/Albert Supp. at 12.

[2233] *Id.* at 12-13.

[2234] *Id.* at 11.

[2235] *Id.* at 12.

[2236] *Id.* at 11.

[2237] *Id.* at 13 (citing PRESERVING VIRTUAL WORLDS REPORT at 6).

[2238] *Id.* at 13-14.

because "[f]or most games where developers have discontinued support, there is no longer a significant market."[2239] They additionally claim that newer games—including "sequels" to discontinued games—are typically quite different from the older titles and are not comparable market substitutes.[2240] EFF/Albert contend that an exemption would actually benefit the market for games "by protecting [a] consumer's investment" in a video game, which will increase its initial value.[2241] Supporting party eBay concurs, adding that the value of video games "plummets without justification if those games can no longer be used because of digital access controls that serve no copyright purpose."[2242]

EFF/Albert do not identify any additional considerations to be weighed under the fifth factor. But, in responding to opponents' concerns, which are further described below, EFF/Albert argue that concerns over diminishment of brand value, safety and privacy, or diminishment of sales of new games within the same franchise (*e.g.*, new "Super Mario Brothers" games) have "no bearing" in this proceeding and are more properly the subject of the trademark, contract, or competition laws.[2243]

2. Opposition

Class 23 is opposed by ESA and Joint Creators.[2244] ESA points out that the video game industry is "one of the fastest growing sectors in the U.S. economy" and has generated over $21 billion in revenue in 2013.[2245] ESA also observes that video games can frequently cost over $50 million to develop, with some costing over $100 million.[2246] They argue that an exemption would threaten this investment in innovation and economic growth.

As an overarching matter, ESA argues that the scope of the class, as proposed, "affects an overly broad range of devices and platforms" and that "granting the request would be incompatible with congressional intent that exemptions be afforded only in the most 'exceptional' cases."[2247] ESA further contends that proponents' understanding of the technology and access controls at issue is inaccurate. According to ESA, "to eliminate authentication checks and enable the video game to be played on a video game console or other device connected to a third-party multiplayer game server . . . would

[2239] *Id.* at 14; *but see* Tr. at 175:15-17 (May 20, 2015) (Albert) (Gamers "would gladly pay huge amounts of money to be able to play these games online again.").

[2240] EFF/Albert Supp. at 14-15.

[2241] *Id.* at 14.

[2242] eBay Class 23 Reply at 1.

[2243] EFF/Albert Reply at 15-16.

[2244] The trade groups represented by Joint Creators are ESA, the Motion Picture Association of America, Inc., and the Recording Industry Association of America.

[2245] ESA Class 23 Opp'n at 1-2.

[2246] *Id.* at 2.

[2247] *Id.* at 5, 7.

require circumvention of a much broader array of video game and device-based access controls" and "would, in effect, eviscerate virtually *all* forms of access protection used to prevent video game piracy."[2248] ESA also takes issue with the proposed exclusion of games that feature "persistent worlds," asserting that proponents created a "false distinction" that "does not correspond to how video games are distributed in practice."[2249] Contrary to EFF/Albert's assumption that the content of such games is stored remotely, ESA states that "[m]ost of the content for the 'persistent world' games that EFF[/Albert] mentions, including World of Warcraft, is actually stored locally to improve the gameplay experience."[2250]

a. Asserted Noninfringing Uses

Class 23 opponents believe proponents have not met their burden to show that circumvention will facilitate noninfringing uses. First, for preservationist uses, opponents argue that the proposed class as written will be used by some to shield infringing conduct.[2251] ESA concedes that preservation, research, and study "sometimes are permitted as fair uses" and did not directly challenge proponents' claim that some proposed preservation activities would be noninfringing.[2252] But ESA argues that the proposed exemption is principally aimed at "enabl[ing] continued single- and multi-player gameplay" with only "*indirect* benefits for video game preservation, research, and study."[2253] ESA argues that the proposed class as written will lead to infringing conduct because, even if expressly limited to preservation uses, "organizations and individuals . . . likely would try to use the guise of 'preservation' or 'research' to make [video games] available for free to the public to play online purely for entertainment purposes [and] regardless of whether they ever purchased a lawful copy of the video game."[2254] Joint Creators agree, stating that "[a]lthough EFF tries to couch the proposed exemption as one that benefits scholars, researchers and preservationists, it is clear that EFF's primary goal is to legitimize game, console, and server hacking for the purpose of enabling casual use of entertaining, copyrighted video games across a wide swath of platforms and devices."[2255]

[2248] *Id.* at 8; *see also id.* at 3 ("[T]here is no such thing as specific access controls that check 'authentication servers' and 'matchmaking servers' for video games . . . . Many of these access controls serve a protective function that is far broader than 'authentication' or 'matchmaking.'").

[2249] *Id.* at 7.

[2250] *Id.* As noted above, EFF/Albert subsequently clarified that they only needed to hack consoles for preservation uses. Tr. at 204:01-03 (May 20, 2015) (Albert); *id.* at 255:01-03 (Stoltz, EFF).

[2251] ESA Class 23 Opp'n at 12-13.

[2252] *Id.* at 12; *see also* Tr. at 212:20-22 (May 20, 2015) (Williams, Joint Creators) ("I am not sure that all of the types of preservation that [proponents are] discussing would ultimately be lawful . . . .").

[2253] ESA Class 23 Opp'n at 10-11 (emphasis added).

[2254] *Id.* at 12-13 (emphasis omitted).

[2255] Joint Creators Class 23 Opp'n at 5.

Next, Class 23 opponents disagree that continued gameplay uses are likely to be noninfringing under section 107. First, reviewing the purpose and character of the use, opponents explain that the proposed use is commercial and not transformative, because "[t]here is abundant evidence that one of the primary reasons many users seek to hack the video game access controls is not to create new and different works, but to avoid paying the customary cost of existing works and devices."[2256] As Joint Creators put it, "the purpose of EFF's [creation of] derivative works is to replicate exactly the same entertainment experience that the games were initially designed to enable while multi-player functionality continues to be offered."[2257] Opponents distinguish the *Sega* and *Connectix* cases cited by proponents, pointing out that, unlike in those cases, users of the exemption would not be "develop[ing] new, expressive works of authorship."[2258]

Under the second fair use factor, opponents argue that the nature of the work does not support fair use, because video games are highly expressive and "entitled to the greatest protection." [2259] Moreover, circumventing the TPMs at issue "necessarily enables and is almost always coupled with" piracy.[2260] Under the third factor, ESA asserts that the amount and substantiality of the portion used is not reasonable, as depending on the device and TPM, the amount of the work copied "could potentially be virtually all of the code for the copyrighted video game."[2261]

ESA focuses much of its argument on the fourth fair use factor, regarding the effect on the market for or potential value of the copyrighted works. ESA notes that "video game publishers routinely re-introduce video games that otherwise would be deemed 'abandoned' under the proposed exemption" and claims that an exemption for gamers would harm that potential market.[2262] In addition, it explains that "many video game publishers improve on prior versions to develop new video games within a franchise," and that granting the exemption could cannibalize sales of such new releases.[2263] Finally, it claims that if hacked games performed poorly or chat functions were unmoderated, this would diminish the value of the game publishers' brands.[2264]

ESA raises particular concerns about the application of this exemption to console-based games and the impact on the market for such games. It states that allowing circumvention to access a video game on a console necessarily "requires hacking of the

[2256] ESA Class 23 Opp'n at 13.

[2257] Joint Creators Class 23 Opp'n at 3.

[2258] ESA Class 23 Opp'n at 13; Joint Creators Class 23 Opp'n at 4.

[2259] ESA Class 23 Opp'n at 14.

[2260] *Id.*

[2261] *Id.* at 15.

[2262] *Id.* at 16; *see also* Joint Creators Class 23 Opp'n at 4.

[2263] ESA Class 23 Opp'n at 16.

[2264] *Id.* at 16-17.

video game console as well."[2265] If a console is hacked, opponents claim, it will not only play the "abandoned" games that would fall under this class, but could also be used to play any pirated video game or make infringing copies of other copyrighted content.[2266] Indeed, ESA provides specific evidence establishing a link between hacking consoles and piracy of copyrighted works.[2267] Pointing to the Librarian's decision in the prior rulemaking to deny an exemption to permit jailbreaking of video game consoles, opponents assert that granting this exemption would lead to hacked consoles that "could no longer serve as a secure method for the development and distribution of legitimate content," including non-video game content such as movies.[2268] If such secure distribution platforms are hacked, opponents claim, "publishers will be *less* likely to make their content available and there will be *less* legitimate content available."[2269]

b. Asserted Adverse Effects

Class 23 opponents believe there are sufficient marketplace alternatives to mitigate or eliminate any adverse effects when server support for a video game ends. Opponents maintain that when video game servers are taken offline, the "vast majority" of games can continue to be played in single-player mode, and users can still enjoy multiplayer modes by using a local area network.[2270] Opponents also contest EFF/Albert's position that users are entitled to continued game play, contending that online services such as multiplayer game play are separate services that are not included in the purchase price of video games.[2271] In a post-hearing letter, ESA stated that, whether at the point of sale or within the game packaging, consumers have "clear and prominent notice that server support for a game may someday be discontinued."[2272] ESA also submitted specific examples of games that continued to be sold after support for

[2265] *Id.* at 16; *see also* Tr. at 215:07-16 (May 20, 2015) (Frankel, ESA) (noting that "[i]t may be that very early generation consoles did not have to be hacked for [circumvention], but it is the case that more recent ones have" and that "all but the very first Xbox would have to be hacked").

[2266] ESA Class 23 Opp'n at 16.

[2267] *Id.* at 4-5, 21, Exhibit A.

[2268] *Id.* at 15.

[2269] *Id.*; *see also* Joint Creators Class 23 Opp'n at 2 ("This proposed class of works should be rejected because circumvention related to videogame consoles inevitably increases piracy and is detrimental to the secure and trustworthy innovative platforms that videogame publishers and consumers demand.").

[2270] ESA Class 23 Opp'n at 17. A local area network connects different computers in a localized area, such as at a home, office, or school, whereas a wide area network, such as the internet, connects computers running at distant locations.

[2271] Joint Creators Class 23 Opp'n at 5 ("[O]nline network services are generally entirely distinct services for which the user must register, and often pay, separately, and are not included in the purchase of the video game.").

[2272] ESA Class 23 Post-Hearing Resp. at 3. For example, the publisher Electronic Arts ("EA") provides a notice on website product pages and packaging for all of its games that states "EA MAY RETIRE ONLINE FEATURES AFTER 30 DAYS NOTICE POSTED ON www.ea.com/1/service-updates." *Id.*

multiplayer gameplay had already ended, with clear notice on the packaging of that fact.[2273]

ESA asserts that non-play options, such as screen capture of gameplay, are viable alternatives to circumvention for preservation purposes.[2274] It concedes that such a solution may be "non-optimal," but points out that exemptions are only for exceptional cases.[2275] ESA argues that proponents have failed to demonstrate a need for circumvention for archival purposes now or in the next three years. ESA further explains that it, along with its member companies, has partnered with institutions that have sponsored "multiple museum exhibitions and educational initiatives related to video games," including the Smithsonian Institution, further demonstrating a lack of adverse effects.[2276]

c. Argument Under Statutory Factors

Class 23 opponents assert that the statutory factors enumerated in section 1201(a)(1) counsel against an exemption. In considering these factors, opponents stress their belief that, like the proposed exemption for jailbreaking video game consoles in Class 19, an exemption for this class would encourage or enable piracy of both video games and other copyrighted works played on circumvented devices.[2277] In support of this view, ESA submitted documentary evidence, including several screenshots of websites dedicated to jailbreaking popular consoles, showing that many of those who wish to jailbreak a console intend to play pirated video games.[2278]

Considering the first statutory factor, the availability for use of copyrighted works, opponents point to the "tremendous positive impact" that the DMCA-protected access controls have had "on the availability of copyrighted materials through personal computers, video game consoles, smartphones, and mobile devices."[2279] ESA argues that granting the proposed exemption "could disrupt the incentive of platform providers and copyright holders to continue making this copyrighted content available to the public," and that copyright owners "may choose to distribute only lower cost content, terminate innovative network services, digital add-ons, and multi-player functionality, or in some

---

[2273] ESA Class 23 Opp'n at 11, Exhibit C (citing stickers placed on game packaging that read "Online features, including Nintendo Wi-Fi Connection, no longer available" on Pokémon White Version 2 for the Nintendo DS and Mario Kart Wii for the Nintendo Wii).

[2274] *Id.* at 17-18.

[2275] *Id.* at 19.

[2276] *Id.* at 18.

[2277] *Id.* at 20.

[2278] *Id.* at Exhibit A. ESA reiterates its view that for console-based games, the console itself would need to be hacked, explaining that "*one hundred percent of video game consoles that play pirated games are hacked . . . .*" *Id.* at 21 (emphasis in original).

[2279] *Id.* at 20.

cases, not agree to permit distribution of their content at all."[2280] According to ESA, because the access controls at issue encourage the availability of works, this "positive impact far outweighs any minimal adverse impact."[2281]

Regarding the second factor, ESA claims that "[p]roponents failed to provide a single example where a specific video game was unavailable" for nonprofit archival, preservation, or educational uses, and that there are many alternatives for such uses.[2282] Similarly, ESA believes that under the third statutory factor, proponents have not offered any "specific evidence" of a substantial adverse effect related to criticism, comment, news reporting, teaching, scholarship, or research.[2283] ESA notes that it and its members have already "participated in and supported multiple museum exhibitions and educational initiatives related to video games," rendering an exemption for such purposes unnecessary.[2284]

For the fourth factor, ESA repeats its concern that an exemption would encourage piracy through the use of altered video game consoles which, in turn, would diminish the market for and value of copyrighted works.[2285]

Finally, opponents suggest that the fifth factor counsels against granting an exemption. Opponents argue that allowing circumvention would interfere with their ability to manage and control their brands. They explain that unauthorized third party servers could provide a lower-quality gaming experience that could be slow, buggy, and vulnerable to safety and privacy threats.[2286] ESA also asserts that if an exemption were granted, "users would wrongly believe that they can traffic in circumvention tools to hack their video games or engage in wholesale reproduction and distribution of the video game software."[2287]

3. Discussion

The Register notes that all parties in this class seem to appreciate the enormous value of video games to our culture and economy. Proponents make a strong case for the personal impact that games have had on their lives, as well as their desire to continue using these games and share gaming experiences with others. But while the Register recognizes the significant interest of gaming communities in this proposed class, proponents still bear the burden of meeting the statutory criteria for an exemption.

[2280] *Id.* at 20-21.

[2281] *Id.* at 20.

[2282] *Id.* at 21.

[2283] *Id.* at 22.

[2284] *Id.* at 18.

[2285] *Id.* at 22.

[2286] *Id.* at 22-23.

[2287] *Id.* at 22.

As explained above, in making their case for an exemption, proponents address two different groups of users: gamers who wish to continue to play video games they own, and preservationists who want to make the games available for research and study. The evidence for these uses was collected as part of a single class, and some of the evidentiary record is relevant to both concerns. At the same time, it is now clear that the legal analysis differs for the two uses. For that reason, the Register treats the uses separately in the discussion below.

The Register observes that proponents rely on fair use as the basis for the proposed exemption and do not invoke section 117, either for gamers or in relation to the requested preservation uses. Section 117 permits the owner of a copy of a computer program to copy or adapt that program when the copy or adaptation is created as an "essential step" in the utilization of the program in conjunction with a machine and is used in no other manner.[2288] A threshold question, then, with respect to the applicability of section 117 is whether the software under consideration is owned or licensed by the user. In some situations where a user enjoys various incidents of ownership—such as the ability to transfer or destroy the software without permission—the user may be considered the owner of software for purposes of section 117 notwithstanding purported license terms.[2289] The two leading precedents on this question—*Krause v. Titleserv, Inc.*[2290] and *Vernor v. Autodesk, Inc.*[2291]—propose different tests to ascertain whether software is owned as opposed to licensed.[2292] While acknowledging these tests as "useful guideposts," the Register has previously concluded that the state of the law in this area is somewhat uncertain.[2293]

Assuming that in some cases the owners of a video game might also be considered the owners of the software on that copy, it seems that section 117 could be relevant to some of activities in which proponents seek to engage. More generally, section 117 evinces Congress's understanding that reverse engineering and the pursuit of interoperability are favored activities under the law.[2294] Because proponents declined to

---

[2288] 17 U.S.C. § 117(a).

[2289] *See Vernor v. Autodesk, Inc.*, 621 F.3d 1102, 1111 (9th Cir. 2010).

[2290] 402 F.3d 119 (2d Cir. 2005).

[2291] 621 F.3d 1102.

[2292] In *Krause*, the Second Circuit held that formal title was not necessary to demonstrate ownership under section 117, but courts should look to a variety of factors to determine "whether the party exercises sufficient incidents of ownership over a copy of the program to be sensibly considered the owner of the copy." *Krause*, 402 F.3d at 124. By contrast, in *Vernor*, the Ninth Circuit held that "a software user is a licensee rather than an owner of a copy, where the copyright owner (1) specifies that the user is granted a license; (2) significantly restricts the user's ability to transfer the software; and (3) imposes notable use restrictions." *Vernor*, 621 F.3d at 1111.

[2293] *See, e.g.*, 2012 Recommendation at 92.

[2294] *See* COMMISSION ON NEW TECHNOLOGICAL USES, FINAL REPORT 13 (1978) (noting that "a right to make those changes necessary to enable the use for which [the computer program] was both sold and purchased should be provided").

put forth section 117 as a legal justification for the exemption, however, the Register analyzes only fair use.[2295]

a. Noninfringing Uses

i. Continued Play

The Register concludes that, in the case of lawfully acquired PC and console-based video games, the overall record supports proponents' claim that copying and modifying game software to allow for continued play after server support ends are likely to be noninfringing fair uses. As discussed below, however, due to piracy concerns, the record does not support extending the exemption to any jailbreaking of consoles. Further, although EFF/Albert also requested the ability to circumvent TPMs on games designed for handheld devices,[2296] no record was developed concerning such games, and the Register therefore concludes that there is no factual or legal basis to include such games or devices in the exemption.

In reviewing the statutory factors, the Register notes that, as discussed above, the proposed exemption contemplates circumvention of self-contained copies of lawfully acquired games in physical or downloaded formats rather than games that involve shared content hosted by third parties (such as persistent world games) or are accessed via subscription, and that these are critical assumptions in the fair use analysis. The Register's analysis is also limited to games that are rendered wholly unplayable due to the lack of an authentication mechanism; because, for reasons discussed below, the Register finds that proponents have not satisfied their burden with respect to a need for an exemption for continued online multiplayer play, such functionality is not considered in the Register's fair use analysis.

With respect to the first statutory factor, the purpose and character of the use, opponents make a valid point that the proposed uses are not transformative, in that proponents simply want to engage in the same use of the copyrighted work as before—namely, the playing of video games, whether on PCs or gaming consoles. On a related

[2295] Likewise, no party analyzes the applicability of section 1201(f), which permits certain acts of reverse engineering as an exception to the prohibition on circumvention. But the Register notes that the provision would not likely protect all of the activities at issue here, and consequently does not obviate the need for an exemption. While the proposed exemption is directed at providing for the continued play and preservation of video games, section 1201(f)(1) is limited to circumvention solely for the identification and analysis of program elements necessary for interoperability, and does not address circumvention after that analysis has been performed. *See* 17 U.S.C. § 1201(f)(1). Accordingly, as the Register previously concluded in the context of considering an exemption for jailbreaking of smartphones in 2010 and of video game consoles in 2012, when an exemption is sought to permit anyone to circumvent a TPM—and "not just those who [perform] 'identification and analysis' of programmatic elements"—it creates "significant doubt" as to whether section 1201(f) would apply. 2012 Recommendation at 45 n.212 (citing 2010 Recommendation at 94-95 & n.318).

[2296] EFF/Albert Pet. at 1 (requesting an exemption for "consoles, personal computers *or* personal handheld gaming devices" (emphasis added)).

note, opponents offer the argument that the *Sega* and *Connectix* cases are distinguishable from this situation, because those cases involved intermediate copying to create new expressive works, whereas here proponents simply wish to play existing games.[2297]

As the Register has opined in prior triennial rulemakings, however, "a use need not be transformative . . . to be a fair use."[2298] For example, in the course of recommending an exemption for "jailbreaking" of smartphones in 2012, the Register explained that the first factor may favor fair use where "the purpose and character of the use is noncommercial and personal" and facilitates functionality.[2299] Here, where gamers wish to modify a copy of video game software they have lawfully acquired simply to allow its continued personal use on their own computers—akin to the adaptation exception embodied in section 117—the first factor tends to support a finding of fair use.

Concerning the second factor, the nature of the copyrighted work, the Register agrees with opponents that video games are highly expressive and thus at the core of copyright's protective purposes. At the same time, the copying and modifications at issue are necessary to allow continued legitimate use of the work, and as EFF/Albert note, those modifications only change the "functional aspects of the software, not expressive elements such as graphics or audio."[2300] When the proposed use is understood in that light, the second factor does not necessarily negate a finding of fair use.

As for the third fair use factor, the amount and substantiality of the work used, the record indicates that only a small amount of the video game software code needs to be modified, though the modification process may require the creation of a complete, albeit temporary, copy of the video game software.[2301] In prior rulemakings, the Register has considered an analogous scenario in the context of smartphone jailbreaking to enable interoperability and concluded that the third factor "arguably disfavors a fair use finding" but that "the weight to be given to [the third factor] under the circumstances is slight."[2302] The same conclusion is warranted here.

The fourth factor considers the effect on the potential market for or value of the copyrighted work. As noted, with respect to gamers who wish to continue to play games for which server support has ended, the proposed exemption applies only where the market for the particular version of that game has been essentially vacated by copyright owners. Certainly opponents are correct in asserting their rights to reintroduce games in

[2297] ESA Class 23 Opp'n at 13.

[2298] 2012 Recommendation at 72 (quoting 2010 Recommendation at 95).

[2299] *Id.* at 74.

[2300] EFF/Albert Supp. at 7; *see also* EFF/Albert Reply at 10-11 ("[T]he software that is modified in the process of circumvention is access controls in game firmware. This is software that does not render video or audio content, nor define the physics, rules, or storyline of a game. It is entirely functional rather than expressive.")

[2301] *See* EFF/Albert Reply at 11.

[2302] 2010 Recommendation at 97; *see also* 2012 Recommendation at 73.

the future; however, this fact alone is not dispositive. Not all such games will be reintroduced, and in the few examples provided by opponents, the games were remastered and did not always include the same functionality as the discontinued versions.[2303] Moreover, the record does not establish that gamers who are so strongly connected to a discontinued game that they will seek alternative means to continue to play it will not purchase a reissue if one becomes available.[2304] The Register acknowledges the importance of preserving future markets and investments, but in this instance, the evidence presented by opponents concerning potential markets for discontinued versions of games was scant. As such, on the present record, the Register concludes that opponents have failed to demonstrate that the market for reissued games would be materially impacted by the proposed exemption.

Class 23 opponents make a stronger case that granting the exemption would cause market harm to the extent it would include jailbreaking of video game consoles by individual users. As explained above, for purposes of the requested exemption as it would apply to gamers, proponents disclaimed a need to circumvent console software in addition to the game itself.[2305] In light of the importance of the issue, however, the Register addresses the console question.

Opponents' concerns are directed to the role of consoles as a secure distribution platform for video games and other copyrighted works. While the Register finds that circumventing discontinued console-based video games themselves, as well as PC games, is unlikely to harm the market for or value of those copyrighted works, the same does not hold true for the value of the gaming consoles on which they are played.[2306] Based on the record (and as discussed in more depth with respect to the proposed exemption to allow console jailbreaking in Proposed Class 19), jailbroken consoles are strongly linked to piracy of video games.[2307] As noted above, a jailbroken console can be used to play

[2303] *See* ESA Class 23 Post-Hearing Resp. at 1-3.

[2304] *See* Tr. at 175:15-17 (May 20, 2015) (Albert) (noting that gamers "would gladly pay huge amounts of money to be able to play these games online again"). It seems also plausible that these gamers would buy updated versions of the game.

[2305] In part this appears to be due to the fact that the exemption focuses on older games, which the record indicates have separate TPMs for authentication and matchmaking purposes that do not affect console play. *See, e.g.*, *id.* at 204:25-205:13 (Stoltz, EFF) ("[M]y understanding is it's much more common that it is the norm with older consoles like the PlayStation 2 that the preservation work can be accomplished without essentially removing all of the anti-piracy features of the console.").

[2306] As noted above, EFF/Albert assert that some older game consoles would not necessarily need to be jailbroken to engage in the circumvention contemplated by the proposed exemption. *See id.* at 173:22-174:03 (Damle, USCO; Albert); *id.* at 202:25-203:08 (Albert). Though proponents seek an exemption that would allow jailbreaking of consoles when necessary for preservation purposes, the record indicates they are not seeking to authorize console jailbreaking by gamers. *See id.* at 255:01-03 (Stoltz, EFF); *id.* at 203:18-204:03 (Charlesworth, USCO; Albert).

[2307] ESA Class 23 Opp'n at Exhibit A; *see also Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 590 (1994) (market harm requires considering "whether unrestricted and widespread conduct of the sort engaged in by the [proponent of fair use] . . . would result in a substantially adverse impact on the potential market" (citations omitted)); 2012 Recommendation at 42-43.

illegitimately acquired games and not just "abandoned" games. Moreover, jailbreaking of console software weakens the efficacy and value of that software as a distribution platform.[2308] The Register therefore concludes that any exemption that would extend to modification of console computer code by individual consumers is likely to cause market harm to the console platform software as well as the non-discontinued games distributed for that platform, and is therefore unlikely to be a fair use.

In sum, because factors two and three are less salient considerations in this context, the fair use analysis tends to favor proponents' desire to engage in continued personal gameplay, except with respect to console jailbreaking activities.

ii. Preservation

The Register next considers whether engaging in circumvention activities to maintain video games in playable condition and make them available for research and study is likely to be a fair use under section 107.[2309] In so doing, the Register notes that Class 23 opponents agree with proponents that preservation, research and study "sometimes are permitted as fair uses."[2310] Indeed, the record demonstrates that ESA and its members actively support research and preservation efforts.[2311]

The consensus evaporates, however, when considering the types of activities and actors properly considered as engaging in "preservation." Proponents take a broad view in which preservation activities overlap with a mere opportunity for continued play, with EFF's representative explaining, "I don't think there is a strong line of demarcation" between preservationists and "someone who [] wants to keep playing the game."[2312] At the public hearing, EFF and Albert sidestepped attempts to more clearly define the contours of the requested preservation activities,[2313] while ESA observed that "[a]s

[2308] ESA Class 23 Opp'n at 9; Joint Creators Class 23 Opp'n at 2.

[2309] As explained above, proponents do not cite section 117 as a basis for granting an exemption, although the Register notes that section 117 permits the owner of a computer program to make a copy for archival purposes. 17 U.S.C. § 117(a)(2). But as with continued play, the record does not establish whether preservationists are likely to be considered "owners" under section 117.

[2310] ESA Class 23 Opp'n at 12.

[2311] Tr. at 234:07-235:17 (May 20, 2015) (Frankel, ESA).

[2312] *Id.* at 241:15-21 (Stoltz, EFF; Charlesworth, USCO); *see also id.* at 232:25-233:02 (Albert) ("I would like to think that [gamers who congregate online for purposes of continued play] are preserving at the same time that they are playing multiplayer online."); EFF/Albert Supp. at 9; Tr. at 240:18-241:02 (May 20, 2015) (Stoltz) ("I want to emphasize this synergy between volunteer efforts by passionate fans and players and professional researchers, archivists and librarians, because the very important work of preservation and archival depends . . . on the volunteer efforts of people who know a game best and who commit many hours of unpaid labor to restoring it and, of course, preserving the physical media.").

[2313] Tr. at 241:15-242:08 (May 20, 2015) (Stoltz, EFF; Charlesworth, USCO) (explaining that EFF does not "think there is a strong line of demarcation [between preservationists and gamers] because there [is] a synergy," in that the efforts of individual gamers supplement the activities of preservationists).

defined by proponents here, preservation is equivalent to being able to play by those who wish and that is not normally what we mean by preservation."[2314]

The Register finds that proponents have not offered persuasive legal support for the proposition that anyone who seeks to continue playing a video game should be treated as a *de facto* preservationist. For example, proponents' view would seemingly blur the concept of preservation with a general exemption for the creation of backup copies, which the Register has repeatedly declined to recommend in the "space-shifting" context.[2315] In copyright law, preservation uses are treated differently from general, all-purpose uses.[2316] The task remains, then, to determine whether the record here supports a narrower category of preservation-related uses that are likely to be noninfringing.

Though it does not address the full range of preservation-related activities advocated by proponents, section 108 of the Copyright Act, which exempts certain activities of libraries and archives, is helpful to this inquiry. Section 108 permits certain reproductions of copyrighted works for purposes of preservation and replacement, and when a format has become obsolete, thus highlighting Congress's recognition of preservation as an important social activity.[2317] But this recognition is balanced with specific limitations on the making of such reproductions, reflecting Congress's acknowledgment of copyright owners' concern over unrestricted copying under the guise of preservation.[2318] Moreover, section 108 applies only to libraries and archives with collections that are either open to the public or "available not only to researchers affiliated with the library or archives or with the institution of which it is a part, but also to other persons doing research in a specialized field."[2319] And while section 108 permits limited distribution of copies to other libraries and archives, such copies are not to be made available to the public in digital formats "outside the premises of the library or archives."[2320] In addition, a library or archives seeking to avail itself of section 108 must not make a reproduction of a copyrighted work for "any purpose of direct or indirect commercial advantage."[2321] Finally, section 108 addresses only the rights of reproduction

---

[2314] *Id.* at 243:18-22 (Frankel, ESA); *see* ESA Class 23 Opp'n at 12-13.

[2315] *See* Tr. at 244:05-09 (May 20, 2015) (Tonsager, ESA); 2012 Recommendation at 157-66. As discussed above in connection with Classes 8 and 10, in this rulemaking, the Register again declines to recommend exemptions for purposes of creating backup copies of audiovisual works and e-books.

[2316] Tr. at 252:08-10 (May 20, 2015) (Charlesworth, USCO); *see also* 17 U.S.C. § 108.

[2317] *See* 17 U.S.C. § 108; H.R. REP. NO. 94-1476, at 74-75 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5688-89; *see also Preservation and Reuse of Copyrighted Works: Hearing Before the Subcomm. on Courts, Intellectual Prop., and the Internet of the H. Comm. on the Judiciary*, 113th Cong. 2 (2014) (statement of Jerrold Nadler, Ranking Member, Subcomm. on Courts, Intellectual Prop., and the Internet) (noting that "[r]ecognizing the unique public service mission served by libraries and archives, Congress first enacted section 108 in 1976, allowing these entities a limited exemption for preservation").

[2318] *See* H.R. REP. NO. 94-1476, at 75.

[2319] 17 U.S.C. § 108(a)(2).

[2320] *Id.* § 108(b)-(c).

[2321] *Id.* § 108(a)(1).

and distribution in the context of preservation-related activities, and does not authorize or except the public performance or display of copyrighted works, except for certain works in their last twenty years of copyright protection.[2322]

The Register finds that section 108 provides useful and important guidance as to Congress's intent regarding the nature and scope of legitimate preservation activities, and hence the types of uses that are most likely to qualify as fair in this area.[2323] Section 108 suggests that such activities should be carried out by a preservation-oriented institution—a library or archives—and, as noted, must not be for direct or indirect commercial gain.[2324] While section 108 is limited to libraries and archives, the record here reflects that museums engage in similar efforts to preserve video games. In light of their similar preservation mission in this context, the Register sees no reason to exclude museums from the reach of the proposed exemption.[2325]

The Register also narrows her consideration of fair use to reproductions and modifications of video game and console software made for the purpose of preserving games in playable condition to enable research and study. Although proponents also seek the ability to modify video games and consoles so they can be exhibited to the public in playable form—undoubtedly an appealing prospect for many—it is important to recognize that these additional uses also implicate the exclusive section 106 rights of public performance and display.[2326] The performance and display of a video game for visitors in a public space is a markedly different activity than efforts to preserve or study the game in a dedicated archival or research setting. Neither proponents nor opponents in this proceeding addressed legal questions relating to the performance or display of video games in museum galleries or similar public venues. Nor did proponents provide factual detail as to the particulars of the exhibitions being proposed. For example, would visitors' interactions with the games be limited in some way, or would visitors be permitted to play games for extended periods of time?

[2322] *See generally id.* § 108. There are other provisions that may come into play but were not discussed in this proceeding. Sections 109 and 110 of the Copyright Act set forth certain exceptions for the display, and the display and public performance of copyrighted works, respectively, but they do not specifically address the preservation uses at issue here. *See id.* § 109(c) (permitting public display of certain works); *id.* § 110 (permitting certain public performances and displays of works).

[2323] While articulating express exceptions for the activities of libraries and archives, section 108 also preserves fair use. *Id.* § 108(f)(4) ("Noting in this section . . . in any way affects the right of fair use under section 107 . . . .").

[2324] *See id.* § 108(a)-(c); *see also* H.R. REP. NO. 94-1476, at 74 (stating that "[u]nder this provision, a purely commercial enterprise could not establish a collection of copyrighted works, call itself a library or archives, and engage in for-profit reproduction and distribution of photocopies").

[2325] *See* EFF/Albert Supp. at 8-9 (referencing efforts by the Strong Museum of Play); *id.* at App. 1-3 (Statement of Alex Handy, The Museum of Art and Digital Entertainment); Antonelli (cited in EFF/Albert Supp. at 8 n.52); *Video and Other Electronic Game Collections* (cited in EFF/Albert Supp. at 8 n.53); MUSEUM OF ART AND DIGITAL ENTERTAINMENT: ABOUT US (cited in EFF/Albert Supp. at 8 n.54); PARS Reply at 2 (describing two exhibitions of modified video games that were displayed on-site).

[2326] 17 U.S.C. § 106(4), (5).

As explained above, the party seeking the exemption has the burden of supporting its request with evidence and legal argument. Although they did not raise it, proponents might have referenced section 109(c) of the Copyright Act, which permits owners of lawfully made copies of works to display them publicly without permission of the copyright owner, "either directly or by the projection of no more than one image at a time, to viewers present at the place where the copy is located."[2327] While section 109(c) would seemingly cover the display of a video game in a museum or other public setting, it does not address the right of public performance, which would also be implicated, as video games render visual images and accompanying sounds.[2328] There is no express exception in the Copyright Act that would appear to address the performance aspects of the exhibition uses at issue here.[2329] The Register expresses no opinion on whether the exhibition activities proposed by proponents, insofar as they constitute public performances, would or could constitute fair or otherwise noninfringing uses of video games or associated console software. The Register merely concludes that the lack of any legal or evidentiary record on this issue precludes such a finding.[2330] More broadly, the lack of a sufficient record requires that the proposed exhibition uses be excluded from the fair use analysis.

Keeping the above in mind, consideration of the individual fair use factors supports a conclusion that the reproduction and modification of functional aspects of video game and console software to enable noncommercial preservation and research activities at qualified institutions are likely to be fair uses. First, the purpose and character of the use—preservation of a video game in playable form for research and study—are favored purposes under section 107.[2331] For the second factor, the nature of the copyrighted work, the works at issue include highly expressive elements, but the focus of the copying is on functional aspects of those works. For the same reasons as explained above in connection with gamers' desire to engage in continued play of discontinued works, this factor does not weigh heavily against fair use. For the third

[2327] *Id.* § 109(c).

[2328] Under section 101 of the Copyright Act, to "perform" a work means "to recite, render, play, dance, or act it, either directly or by means of any device or process or, in the case of a motion picture or other audiovisual work, to show its images in any sequence or to make the sounds accompanying it audible." *Id.* § 101.

[2329] *See generally id.* §§ 109, 110. Section 109(e) provides an exception to the performance and display rights for "electronic audiovisual game[s] intended for use in coin-operated equipment," but this would not seem to apply to the non-arcade uses proponents are requesting. As explained above, proponents failed to provide details concerning the exhibition activities they proposed; at no point did they suggest the use of coin-operated machinery in connection with these activities.

[2330] These may be appropriate issues for consideration in a future rulemaking proceeding. In addition to addressing fair use under section 107, a legal analysis of the proposed exhibition uses might also consider the potential relevance of sections 109 and 110 of the Copyright Act, which set forth certain exceptions to the rights of public performance and display.

[2331] *See id.* § 107 ("[T]he fair use of a copyrighted work . . . for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright.").

factor, the amount and substantiality of the work used, as also explained above, even though the entire work may be copied and used in modified form, because these uses are aimed at the functional rather than the expressive aspects of the work, this factor also carries little weight.

With respect to the fourth fair use factor, allowing circumvention by appropriate entities solely for noncommercial preservation and research purposes—without distribution to or offsite access by members of the public, consistent with section 108—would not appear to carry a significant risk to the market. Opponents have made no showing of market harm resulting from existing efforts of libraries, archives or museums to preserve video games. Indeed, the record demonstrates that video game developers have in fact cooperated with various institutions to facilitate these activities.[2332]

Although they did not specify why, proponents appear to view the ability to jailbreak video game consoles as more critical for preservationists—perhaps this is to ensure that efforts to preserve games played on more modern consoles are not impeded.[2333] As explained above, opponents point to a strong connection between console jailbreaking and video game piracy. As also discussed above, the Register credits this concern and recommends against allowing console jailbreaking by gamers generally. The Register nonetheless observes that in the case of preservation activities, libraries, archives and museums are a far more confined class than gamers at large, and the proposed uses would be limited to on-site activities in a controlled environment. The risk of piracy would therefore appear to be greatly diminished in the preservation context. Indeed, the record does not reflect any instances of piracy attributable to video game preservation activities. Accordingly, the Register concludes that in the case of video games that have lost outside server support and cannot be accessed for any type of play, the fourth factor weighs in favor of permitting continued access and gameplay of PC and console-based games, as well as copying and modification of console software to the extent necessary to activate an unsupported console game.

On the whole, looking primarily to the first and fourth factors, the Register finds that the fair use analysis tends to favor proponents in relation to the preservation uses.[2334]

b. Adverse Effects

i. Continued Play

To support the claim of adverse effects for gamers, proponents make various claims related to consumers' expectations regarding video games they purchase. For

[2332] *See* ESA Class 23 Opp'n at 18 (referencing ESA partnership with Smithsonian).

[2333] *See* Tr. at 204:20-23 (Stolz, EFF) (noting that "it is probably more common on the current generation of consoles that restoring the game to functionality will require jailbreaking of the console").

[2334] Again, for the reasons discussed below, because the Register finds that proponents have not satisfied their burden with respect to a need for an exemption, this fair use finding does not extend to online multiplayer play.

example, EFF/Albert state that "server shutdowns degrade or destroy the value of a consumer's investment in a game."[2335] With respect to authentication processes, as explained above, the record suggests that some games require a connection to an external server—sometimes on an ongoing basis—for all types of play, including single-player play.[2336] When a server shutdown blocks even single-player play, consumers lose access to the work they have purchased.[2337] Thus, to the extent the prohibition on circumvention prevents modification of the game to allow any type of continued play, the record here supports the conclusion that the prohibition adversely affects gamers.

A different conclusion is warranted for multiplayer matchmaking servers. The ability to engage in online multiplayer play is a functionality that extends beyond the game or TPM itself. Unlike an authentication check, matchmaking functionality involves not just the operation of a TPM, but also the service of connecting one player to other players over the internet (as well as sometimes providing downloadable content, leaderboards, badges, chat, and other social features).[2338] If a matchmaking service is discontinued, the loss of online multiplayer play through that service is not caused by the TPM; circumventing the TPM cannot restore the service. What proponents in fact seek to do is circumvent for the purpose of implementing a *new* external service, which is somewhat different than accessing the game itself.

Moreover, Class 23 opponents make a strong case that when matchmaking support ends, there are alternatives to circumvention. They explain that in most cases, gamers can still engage in one or more of the following: single-player play, multiplayer play at one location using one device and multiple controllers, or multiplayer play using a local area network.[2339] In other words, the game is still accessible and still playable in multiplayer mode.

[2335] EFF/Albert Reply at 14.

[2336] *See* EFF/Albert Supp. at App. (table listing game server shutdowns in 2014, including four games where server connections were required for all play); *id.* at 11; EFF/Albert Reply at 9.

[2337] EFF/Albert Supp. at 14.

[2338] ESA Class 23 Opp'n at 8. Significantly, as noted above, opponents point to examples of disclaimers included on the packaging of video games that make clear that multiplayer support will be offered only for a limited time by license, or may even be discontinued by the time the game is purchased. *Id.* at 11, Exhibit C.

[2339] There may also be other means to enable remote multiplayer play that do not require circumvention. At the public hearing, EFF referred to a service called GameRanger that facilitates multiplayer play of older games over the internet, apparently without the need to modify the game itself, although it is unclear whether such services have or need licenses from game publishers. *See* Tr. at 205:14-19 (May 20, 2015) (Stoltz, EFF) (discussing GameRanger service); *id.* at 231:03-15 (Gholami, Azentium) (same); *see also Games*, GAMERANGER, http://www.gameranger.com/games (cited in EFF/Albert Supp. at 5 n.22) (listing 723 games it supports for PC and Macintosh platforms). EFF/Albert also refer to software called XBConnect that "uses the local network play functionality in some games to allow for play over the Internet, often called 'tunneling.'" EFF/Albert Supp. at 5. Without further details about these services, it is not possible to definitively determine on the record at hand whether these services indeed can operate without circumventing TPMs.

In addition, the Register is concerned that circumvention for multiplayer play could implicate the anti-trafficking provision of section 1201(a)(2), which provides in pertinent part that "[n]o person shall . . . otherwise traffic in any technology, product, service, device, component, or part 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."[2340] Reinstating multiplayer play may require not only replicating or creating new protocols that communicate with games, but also launching a new centralized server and distributing the new protocols to gamers.[2341] It is far from clear to the Register that these activities would be consistent with the anti-trafficking limitations of section 1201(a)(2), which are not subject to waiver through the triennial proceeding.[2342]

For these reasons, while proponents have established that the prohibition on circumvention in section 1201(a)(1) is likely to have adverse effects on gamers' ability to engage in continued personal gameplay when support for a server that performs a necessary authentication check for any type of play has ended, they have not met that burden in the case of discontinuation of developer support for online multiplayer play.

ii. Preservation

To the extent that the shutdown of an authentication server bars access to a video game entirely, the record demonstrates that efforts to preserve video games will likely be impeded by the prohibition on circumvention.[2343] The Register agrees with proponents that screen capture, which makes an audiovisual recording of the game in operation, is not adequate to mitigate the adverse effects on preservationists, who rightfully may seek to preserve playable versions of games.[2344]

But as was true in the case of continued play by gamers, the Register reaches a different conclusion with respect to circumvention to achieve multiplayer play through an external matchmaking server. In addition to the analysis presented above, the Register notes that the record does not demonstrate that preservationists need to replicate online matchmaking servers if the objective is preservation of the game in playable form for future research and study. First, as explained above, section 108 suggests that preservation activities are properly limited to on-site uses, and multiplayer play over the

[2340] 17 U.S.C. § 1201(a)(2)(A).

[2341] *See* EFF/Albert Supp. at 4-6.

[2342] *See* 17 U.S.C. § 1201(a)(2)(A); *see also id.* § 1201(a)(1)(E) ("Neither the exception under subparagraph (B) from the applicability of the prohibition contained in subparagraph (A), nor any determination made in a rulemaking conducted under subparagraph (C), may be used as a defense in any action to enforce any provision of this title other than this paragraph.").

[2343] *See, e.g.*, EFF/Albert Supp. at App. (Statement of Jason Scott, Internet Archive) (describing the need for circumvention).

[2344] *Id.* at App. (Statement of T.L. Taylor, Massachusetts Institute of Technology) ("The preservation of computer games includes not only making sure we can see their graphics or hear their sounds, but understand the complexity of their mechanics . . . .").

internet would violate that principle. Moreover, the objective of permitting researchers to experience multiplayer play would appear to be satisfied by the alternatives to circumvention put forward by opponents, namely, by connecting multiple controllers to a single device or using local networking capabilities.[2345]

c. Statutory Factors

The Register finds that the statutory factors support an appropriately limited exemption to facilitate both continued personal gameplay and preservation activities.

i. Continued Play

With respect to games that depend upon a server-based authentication check for which developer support has been discontinued, the Register concludes that the first statutory factor—the availability for use of copyrighted works—weighs in favor of granting an exemption. As explained, when a video game developer ends support for an authentication server necessary to play a particular game owned by a consumer, the consumer loses all access to that copyrighted work. Granting the exemption would allow consumers to restore access to lawfully acquired games, thus enhancing the availability of copyrighted works.[2346]

The second and third statutory factors, which consider the availability for use of works for nonprofit archival, preservation, and educational purposes and the impact the prohibition on the circumvention has on criticism, comment, news reporting, teaching, scholarship, or research,[2347] are not especially relevant to the analysis of continued play. Gamers' desire to pursue continued gameplay appears primarily motivated by the entertainment value of the games rather than a desire to engage in criticism or pedagogy.

Considering the fourth factor, the effect of circumvention on the market for or value of copyrighted works,[2348] the analysis is similar to that under the fourth fair use factor. Although, in the context of continued gameplay, proponents appear to concede that console jailbreaking is unnecessary, in analyzing market impact, opponents focus their arguments on the harms of such jailbreaking and associated piracy. As discussed above, the Register agrees that granting an exemption permitting gamers to engage in console jailbreaking could adversely affect the market for copyrighted works, including the value of the console software as an effective distribution platform. Setting aside jailbroken consoles, however, there was no specific evidence to show that granting an

[2345] Though perhaps suboptimal, screen capture can be used to supplement preservation and exhibition efforts for multiplayer play.

[2346] In light of the finding that the threshold criteria for an exemption to allow continued online multiplayer play have not been satisfied, the Register declines to analyze this aspect of the proposal under the statutory factors.

[2347] 17 U.S.C. § 1201(a)(1)(C)(ii)-(iii).

[2348] *Id.* § 1201(a)(1)(C)(iv).

exemption would adversely affect the market for video games. Accordingly, outside of the context of jailbroken consoles, the fourth factor favors plaintiffs.

Under the fifth factor, which includes such other considerations as the Librarian considers appropriate,[2349] opponents claim an exemption could harm their brands, and that users of an exemption will be susceptible to security risks and software bugs. While some of these concerns may be legitimate, without more evidence in the record to support them, they appear too speculative to weigh against an exemption. Opponents also worry that some users might misinterpret an exemption for continued play as extending to trafficking in circumvention tools. As detailed above, the Register has taken trafficking concerns into account in considering the proposed class.

ii. Preservation

Under the first statutory factor, the Register concludes that a relatively narrow exemption, drawing upon some of the principles of section 108, would allow libraries, archives and museums to restore and maintain access to video games that might otherwise be lost, thus enhancing the availability of copyrighted works. Such preservation efforts may also stimulate new copyrighted works offering commentary and analysis of video games.

Regarding the second factor, which considers the availability for use of works for nonprofit archival, preservation and educational purposes, the record clearly favors granting the exemption.[2350] Similarly, on the current record, the third statutory factor, the impact of the prohibition on circumvention on criticism, comment, news reporting, teaching, scholarship, or research, weighs heavily in favor of granting the exemption. EFF/Albert provide substantial evidence that the prohibition on circumvention inhibits scholars from accessing older works and replicating "the experience of originally playing the game" in order to study game design or construction.[2351] Scholars and others who seek to understand the cultural and design aspects of video games—as well as their research efforts and commentary—will benefit if the games remain available in playable form.

Turning to the fourth factor, the effect of circumvention on the market for or value of copyrighted works, the Register concludes that a properly crafted exemption for preservationists can satisfy their needs without impacting the market for video games. As noted under the fair use analysis, it appears unlikely that jailbreaking of consoles by preservationists in a controlled setting would result in harm to the market for either console software or the video games that run on those consoles.

[2349] *Id.* § 1201(a)(1)(C)(v).

[2350] EFF/Albert Supp. at 13 (citing PRESERVING VIRTUAL WORLDS REPORT at 6).

[2351] *Id.* at 13-14.

Finally, under the fifth factor, again on this record, the brand and security concerns raised by opponents appear too speculative to weigh against an appropriately tailored exemption.

4. NTIA Comments

NTIA supports the adoption of this exemption largely as requested by proponents. Recognizing that the proposal would benefit two separate yet "intertwined" groups, NTIA believes that the record supports an exemption for both continued gameplay and preservation uses.[2352] In NTIA's view, any exemption should authorize circumvention not only for single-player gameplay but also for multiplayer functionality. NTIA asserts that consumers receive inconsistent notice at best that developers may discontinue support for multiplayer use.[2353] NTIA also discounts the utility of LAN-enabled multiplayer play, finding the requirement to be on the same local network to be a "significant limitation compared to the global reach afforded by play over the Internet."[2354]

NTIA believes that the proposed uses are likely to be fair under section 107, stating that a use need not be transformative to be favored under the first factor, "especially when the user is acting to restore the ability to access a work that he or she had originally been allowed to use."[2355] NTIA rejects opponents' view that the exemption could affect the market for sequels or other video games, stating "analysis of the fourth factor should focus on the market for the work at issue and not on the collateral effect on the market for other works."[2356] While acknowledging opponents' concerns that allowing circumvention of TPMs on video game consoles could lead to "widespread piracy," NTIA would nonetheless allow circumvention of consoles for purposes of the proposed exemption, asserting that it "is not likely to contribute significantly to [] piracy."[2357]

NTIA also recommends that any exemption should include personal handheld gaming devices in addition to consoles or PCs, but does not point to any evidence in the record relating to handheld devices.

As explained above, the Register finds that the record supports granting an exemption to cover both continued gameplay and preservation uses, but one more specifically contoured to reflect the evidence submitted. As summarized below, the Register does not agree that the record supports an exemption for online multiplayer play, in part due to trafficking concerns, which NTIA does not address. Additionally, the

[2352] NTIA Letter at 64.

[2353] *Id.* at 64-65.

[2354] *Id.* at 69.

[2355] *Id.* at 66.

[2356] *Id.* at 67-68.

[2357] *Id.* at 68.

record contains strong evidence linking jailbreaking of console software to increased piracy, and so the Register recommends limiting the ability to circumvent TPMs on consoles to preservationist uses only. Finally, as noted above, the Register was unable to consider handheld devices due to the lack of record evidence.

5. Conclusion and Recommendation

For the reasons described above, the Register finds that the evidentiary record supports an exemption for PC and console-based video games to allow continued personal gameplay and preservation activities when developer server support has ended, though one more circumscribed than that described by proponents. As in the past, when there is a basis in the record for some, but not all, of the class, the Register will refine the class definition to ensure it reflects the legal and evidentiary findings.[2358]

To begin with, the Register adopts proponents' two-part test to determine when server support has ended; that is, either the developer has announced the end of server support, or there has been no server support for a period of at least six months.[2359] The Register also adopts proponents' suggestion that the exemption should cease to apply to new acts of circumvention if server support for the game is restored by the copyright owner.[2360]

Proponents' focus is on self-contained copies of physical or downloaded games; as proposed, the exemption is not intended to reach "persistent world" games or subscription-based games. To this end, following EFF/Albert's suggestion, the Register recommends that the exemption exclude uses that require access to or copying of copyrightable content stored or previously stored on developer game servers, finding this to be an important limitation.[2361]

The Register appreciates that there may be a lack of certainty in terms of whether gamers and preservationists are owners or licensees of the copies of the games in their possession. The Register understands that, from a practical standpoint, proponents are speaking of those who lawfully possess physical or downloaded copies of games, regardless of whether the software is legally owned; thus, the Register recommends extending the exemption to such lawful possessors, understanding that they may not be the legal owners of the software copy they possess. The Register concludes that because the exemption is premised on fair use and not dependent upon section 117, the lack of ownership should not be determinative of eligibility for the exemption.

[2358] *See, e.g.*, 2010 Recommendation at 16 (explaining that "in many cases, [an initial] subset of a category of works should be further tailored in accordance with the evidence in the record").

[2359] EFF/Albert Supp. at 3.

[2360] *Id.* at 4.

[2361] Tr. at 228:13-25 (May 20, 2015) (Stoltz, EFF).

As discussed above, the Register has determined that with respect to online multiplayer play, proponents have failed to provide persuasive support for their case. In particular, the harms of which proponents complain appear to flow more from the termination of matchmaking services—which are not part of the copyrighted works—than from the imposition of TPMs controlling access to those services. Moreover, it is not clear on the current record how the provision of alternative matchmaking protocols to multiple users could be accomplished without running afoul of the anti-trafficking provisions of section 1201(a)(2). In any event, the record does show that continued access and use of the video games, including multiplayer play, is still possible using locally connected devices, a reasonable alternative to circumvention.

With respect to gamers at large, the record supports granting an exemption to allow circumvention of TPMs on lawfully acquired PC and console-based video games that require communication with authentication servers when the requisite servers are taken offline. In this scenario, the inability to circumvent the TPM means that all gameplay is precluded, a significant adverse effect. Because the record demonstrates a substantial relationship between jailbreaking of video game consoles and piracy, however, the Register finds that the exemption for circumvention of authentication checks should not encompass the jailbreaking of console software by gamers for purposes of continued gameplay. Indeed, as noted above, proponents have indicated that they are not seeking the ability to jailbreak consoles in this context. As also noted above, proponents have failed to offer any evidence to support an exemption that extends to handheld devices.

The Register additionally finds that the record supports granting an exemption for libraries, archives and museums to allow circumvention of TPMs so that video games can be preserved in playable condition when authentication servers are discontinued. In the case of preservation, since the risks of piracy appear greatly diminished in that context, the exemption should also extend to TPMs controlling access to computer programs used to operate video game consoles, assuming such circumvention is necessary to maintain a console game in playable form.[2362]

The record clearly establishes that libraries and archives, along with museums, engage in valuable preservation activities with respect to video games. It does not, however, support a broader exemption to allow reproductions and adaptations by other types of institutions or individual actors for more general "preservation" purposes. The Register notes, however, that interested individuals may be able to contribute to valuable preservation efforts by lending their talents and expertise to qualified institutions.

Certain limitations set forth in section 108 of the Copyright Act are instructive in defining the appropriate scope of a preservation exemption for video games. As suggested by section 108, the exemption should be limited to institutions that open their

[2362] The Register notes, however, that this piracy concern may not apply to older consoles because they may not need to be circumvented to restore video game functionality. *See* EFF/Albert Reply at 5-6.

collections to the public and/or to outside researchers. Additionally, the activities must be conducted without any purpose of direct or indirect commercial advantage. While the uses may include reproduction and modification of video game and console software necessary to preserve games in playable form, they do not extend to exhibition activities involving public performance or display. And finally, any digital copies or adaptations of the video games or console software created by the institution as a result of preservation efforts must not be distributed or otherwise made accessible beyond the physical premises of the institution.

Accordingly, the Register recommends that the following class of works be exempt from the prohibition on circumvention for the next three years:

(i) Video games in the form of computer programs embodied in physical or downloaded formats that have been lawfully acquired as complete games, when the copyright owner or its authorized representative has ceased to provide access to an external computer server necessary to facilitate an authentication process to enable local gameplay, solely for the purpose of:

(A) Permitting access to the video game to allow copying and modification of the computer program to restore access to the game for personal gameplay on a personal computer or video game console; or

(B) Permitting access to the video game to allow copying and modification of the computer program to restore access to the game on a personal computer or video game console when necessary to allow preservation of the game in a playable form by an eligible library, archives or museum, where such activities are carried out without any purpose of direct or indirect commercial advantage and the video game is not distributed or made available outside of the physical premises of the eligible library, archives or museum.

(ii) Computer programs used to operate video game consoles solely to the extent necessary for an eligible library, archives or museum to engage in the preservation activities described in paragraph (i)(B).

(iii) For purposes of the exemptions in paragraphs (i) and (ii), the following definitions shall apply:

(A) "Complete games" means video games that can be played by users without accessing or reproducing copyrightable content stored or previously stored on an external computer server.

(B) "Ceased to provide access" means that the copyright owner or its authorized representative has either issued an affirmative statement indicating that external server support for the video game has ended and such support is in fact no longer available or, alternatively, server support has been discontinued for a period of at least six months; provided, however, that server support has not since been restored.

(C) "Local gameplay" means gameplay conducted on a personal computer or video game console, or locally connected personal computers or consoles, and not through an online service or facility.

(D) A library, archives or museum is considered "eligible" when the collections of the library, archives or museum are open to the public and/or are routinely made available to researchers who are not affiliated with the library, archives or museum.

L. Proposed Class 24: Abandoned Software – Music Recording Software

1. Proposal

Proposed Class 24 would allow circumvention of a dongle-like access control that is allegedly no longer supported by the developer or copyright owner and protects a specific type of music recording software, Ensoniq PARIS. Three individuals, Richard Kelley, James McCloskey, and Michael Yanoska, filed similar petitions seeking this exemption,[2363] and the NPRM described the proposed class as follows:

> Proposed Class 24: This proposed class would allow circumvention of access controls consisting of the PACE content protection system, which restricts access to the full functionality of lawfully acquired Ensoniq PARIS music recording software.[2364]

According to petitioners, access controls prevent users of Ensoniq PARIS, a digital audio workstation used in the professional audio industry by artists, composers, and sound engineers,[2365] from utilizing their PARIS software and "hav[ing] access to their own original music."[2366] Petitioners suggested that the problem has arisen because Intelligent Devices, the company that created and sold the PARIS software, "refus[es] to provide new PACE response codes to 'unlock' the [PARIS] software," thus preventing "the small group of [PARIS] users still in existence" from using the software purchased by such users on new computers.[2367]

Following the initial petition phase of the proceeding, none of the petitioners submitted legal arguments or evidence or participated in the public hearings in support of their petition. Short comments expressing general support for the proposal were filed by the Music Library Association ("MLA"), the Free Software Foundation ("FSF"), Catherine Gellis and the Digital Age Defense project ("Gellis/Digital Age Defense"), and over 1500 individuals. These comments, however, were written generically to apply to multiple classes, and no commenter provided specific information concerning the PARIS

[2363] Kelley Pet. at 1 (seeking an exemption for "[o]bsolete software/hardware combinations protected by a software based copy protection mechanism (software dongle) when the manufacturer is unable (because of no longer being in business) or unwilling to provide access via this system to those who are otherwise entitled access" or "that prevents the hardware and software from running on current operating systems or current hardware by those otherwise entitled to access to the software and hardware"); McCloskey Pet. at 1 (seeking an exemption for "[c]omputer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete," including the PARIS software); Yanoska Pet. at 1 (requesting "[e]limination of the PACE control on recording software that was created and sold over 15 years ago (which is no longer sold or supported by the creating company)").

[2364] NPRM, 79 Fed. Reg. at 73,870.

[2365] Kelley Pet. at 1-2. The Ensoniq PARIS workstation is a closed system consisting of the PARIS software and audio recording and mixing hardware. *Id.*

[2366] McCloskey Pet. at 2; *see also* Kelley Pet. at 2-3.

[2367] Yanoska Pet. at 1.

software or the PACE system.[2368] Gellis made a statement in broad support of the exemption at the public hearing, but did not provide supporting details or tailor her remarks to the specifics of the proposed class.[2369] The class is opposed by Joint Creators, who raise significant concerns about the lack of supporting evidence, as well as the scope of the proposed exemption, which have not been rebutted.[2370]

2. NTIA Comments

NTIA explains that while it is "generally open to supporting exemptions for obsolete, legally purchased software . . . proponents need to provide sufficient evidence on the record," and that "proponents did not meet that burden in this case."[2371] Accordingly, NTIA concludes that "[w]ithout more evidence in the record to address opponents' arguments and bolster supporting claims, [it] is unable to support the proposed exemption at this time."[2372]

3. Conclusion and Recommendation

In their petitions, Kelley, McCloskey, and Yanoska raise a potentially valid concern that the loss of developer or copyright owner support required to access the PARIS software may result in adverse effects on those trying to make legitimate uses of that software. It is therefore unfortunate that neither they nor any other commenting party followed up with a substantive submission detailing the legal and factual support for the proposal.[2373] In light of the lack of a record to substantiate the requested exemption, the Register cannot recommend adoption of Proposed Class 24.[2374]

[2368] *See* MLA Class 24 Supp. at 1; FSF Class 24 Supp. at 1; Gellis/Digital Age Defense Class 24 Supp. at 1; Battilana Class 24 Supp. at 1; *see also generally* Digital Right to Repair Class 24 Supp. (1530 individuals).

[2369] Tr. at 44:11-45:22 (May 21, 2015) (Gellis, Digital Age Defense).

[2370] Joint Creators Class 24 Opp'n at 3 (finding fault with the claim that the PARIS software, rather than the PACE TPM on the software, is obsolete).

[2371] NTIA Letter at 70 (citing NPRM, 79 Fed. Reg. at 73,857).

[2372] *Id.* at 71.

[2373] *See* 17 U.S.C. § 1201(a)(1)(C); 2012 Recommendation at 8 (explaining the preponderance of the evidence standard).

[2374] The Register notes that if proponents are still interested in accessing the PARIS software, they may wish to contact the responsible companies directly to obtain authorization to circumvent the alleged access controls.

M. Proposed Class 26: Software – 3D Printers

1. Proposal

Proponent Public Knowledge seeks an exemption to permit the circumvention of access controls on computer programs in 3D printers to enable the use of non-manufacturer-approved feedstock in the printers.[2375] The Office understands the term "3D printing" to describe various technologies that translate digital files into physical objects by adding successive layers of material.[2376] 3D printing—also called "additive" manufacturing—can be distinguished from traditional computer-controlled manufacturing, such as industrial CNC mills, lathes, or plasma or laser cutters, which are "subtractive" material removal processes. As proposed, the exemption would apply to both commercial and noncommercial 3D printers.[2377] The NPRM described the class as follows:

> Proposed Class 26: This proposed class would allow circumvention of TPMs on firmware or software in 3D printers to allow use of non-manufacturer-approved feedstock in the printer.[2378]

Comments supporting the proposed exemption were filed by Catherine Gellis and the Digital Age Defense project ("Gellis/Digital Age Defense"), the Free Software Foundation ("FSF") and over 1600 individuals.[2379]

a. Background

The 3D printing industry is growing rapidly. In 2013, worldwide sales for 3D printer systems and materials were $1.5 billion, and are projected to grow to $7 billion in

[2375] Public Knowledge specifically proposed the following: "an exemption for users of 3D printers that are protected by control technologies when circumvention is accomplishes [sic] solely for the purpose of using non-manufacturer approved feedstock in the printer." Public Knowledge 3D Printing Pet. at 2. The Library Copyright Alliance ("LCA") joined Public Knowledge in the initial supporting comments, but not the reply round of comments.

[2376] Public Knowledge/LCA Supp. at 3; *see also* Stratasys Opp'n at 1 ("The proposed class of '3D printers' comprises various technologies that translate digital files into physical objects by adding successive layers of material, sometimes referred to as additive manufacturing.").

[2377] Tr. at 137:19-23 (May 28, 2015) (Weinberg) (explaining "while [Class 26] was originally motivated by focus on consumer use, I don't think there is any reason to exclude manufacturing or more sophisticated commercial players").

[2378] NPRM, 79 Fed. Reg. at 73,871. The Register notes that although the terms "firmware" and "software" are variously used throughout the Recommendation, both are "computer programs" within the meaning of the Copyright Act. *See* 17 U.S.C. § 101 (definition of "computer program").

[2379] Gellis/Digital Age Defense Class 26 Supp.; FSF Class 26 Supp.; Digital Right to Repair Class 26 Supp. (1577 individuals); Gregory Borodiansky Reply; Patrick Brett Reply; Digital Right to Repair Class 26 Reply (123 individuals); Henry Feldman Reply; Patrick Ferguson Reply; Robert Gusek Reply; Alex Hatch Reply; Don Lowery Reply; Matthew Nupen Reply; Michael Weinberg Reply.

2016 and $21 billion in 2020.[2380] The materials or "feedstock" used in a 3D printer can consist of metals, waste plastics, woods, or bio-tissue, but most typically are ABS or PLA plastics.[2381] Manufacturers of 3D printers commonly sell manufacturer-approved feedstock, in part for alleged quality control purposes.[2382] Public Knowledge explains that manufacturers of some 3D printers use TPMs to restrict the types of feedstock that can be used in their 3D printers to authorized feedstock.[2383] Public Knowledge seeks an exemption permitting users to circumvent these TPMs in order to use non-manufacturer-approved feedstock in their 3D printers. This feedstock may be a less expensive version of the same material used by the manufacturer (*e.g.*, ABS plastic with the same chemical composition as manufacturer-approved feedstock) or feedstock composed of a different material (*e.g.*, metal instead of plastic).[2384]

Public Knowledge explains that many TPM systems rely on a microchip attached to a printer feedstock cartridge that allows printer operating system software to verify that the feedstock is manufacturer-authorized before the software allows the printer to print 3D objects.[2385] Although Public Knowledge did not provide specifics, it suggests that in some systems, these microchips may not even control access to a copyrighted work.[2386] Some 3D printer TPMs use "dumb" chips such as radio-frequency identification chips, key cards, or chips that contain serial numbers.[2387] Circumvention of these TPMs is likely to require copying factual information from a verification chip to a third-party chip, or reprogramming an original chip with information about the third-party replacement feedstock.[2388] By way of example, Public Knowledge pointed to the Cube, a home printer manufactured by 3D Systems, which restricts use to only manufacturer-produced feedstock cartridges by verifying the existence of a valid chip on the cartridge.[2389] Other 3D printers use more complex chip-based TPMs, including authentication methods that contain copyrighted software on the chip, but Public Knowledge did not further explain how those TPMs functioned.[2390] Opponent Stratasys, a 3D printer manufacturer,

---

[2380] Stratasys Opp'n at 26 (citing WOHLERS ASSOCIATES, WOHLERS REPORT 2014: 3D PRINTING AND ADDITIVE MANUFACTURING STATE OF THE INDUSTRY 110, 116 (2014) ("WOHLERS REPORT")).

[2381] Public Knowledge/LCA Supp. at 4, 9.

[2382] *See* Stratasys Opp'n at 27-30.

[2383] Public Knowledge/LCA Supp. at 5.

[2384] *Id.* at 9-10.

[2385] Public Knowledge Class 26 Reply at 2; Public Knowledge/LCA Supp. at 5. Public Knowledge declined to provide information about other specific TPMs or circumvention methods. Public Knowledge Class 26 Reply at 1-2.

[2386] *See* Tr. at 127:03-12 (May 28, 2015) (Siy, Public Knowledge); *see also* Stratasys Opp'n at 14; Public Knowledge/LCA Supp. at 6.

[2387] Tr. at 134:19-136:08 (May 28, 2015) (Weinberg; Charlesworth, USCO).

[2388] Public Knowledge Class 26 Reply at 2; Stratasys Opp'n at 9-10.

[2389] Public Knowledge/LCA Supp. at 5.

[2390] Tr. at 185:02-11 (May 28, 2015) (Siy, Public Knowledge) (stating that more sophisticated chip-based TPMs are coming to the market which may require different circumvention methods); *see also id.* at

observed that these "smart" chips can "hold data read by the printer's software" which "generally consists of nonexecuting code that includes information such as the amount of material in the cartridge, the type of material, and the batch number."[2391]

In addition to whatever hardware or software modifications are needed so that a 3D printer will accept non-manufacturer-approved feedstock,[2392] use of feedstock composed of materials other than the material a 3D printer has been designed to use (*e.g.*, metal instead of plastic) may require further modification of the printer's operating system software, for example, to change preset variables such as the rate at which the heated feedstock is extruded to create the object or the temperature of the extrusion nozzle.[2393] Without those modifications, 3D-printed objects using such feedstock may print with errors or not print at all. Stratasys explains that there are TPMs (separate and apart from the chip verification systems) that prevent access to this operating system software, such as "panels, ports, and user names and passwords on the user console," but did not provide further detail or offer examples of printer models that employ these TPMs.[2394]

In addition, Stratasys states that 3D printers may contain "other intellectual property" such as "design software, [computer assisted design or] CAD files, proprietary machine-readable files, and reports compiling performance or other data."[2395] Design software is used to design three-dimensional objects to be printed on a 3D printer; Stratasys acknowledges that this software is typically developed and owned by third parties, not Stratasys, or is available as open source software.[2396] CAD files, in turn, are digital files typically created on a desktop computer that hold the designs of 3D objects; Stratasys notes that such designs may be copyrighted and owned by third-parties.[2397]

133:07-11 (Weinberg) ("You could also structure the system where there is much more information in the feedstock container chip, and so it's a more, instead of a kind of look-and-see structure, the two pieces talk to each other in a much more intensive way.").

[2391] Stratasys Opp'n at 9. Stratasys does not believe that the software on the microchips themselves is protected by copyright, but suggests future versions might be copyrightable. Tr. at 169:09-14 (May 28, 2015) (Riley, USCO; Carey, Stratasys); *id.* at 171:23-172:03 (Carey, Stratasys).

[2392] *See* Tr. at 126:11-16 (May 28, 2015) (Siy, Public Knowledge) ("[U]ltimately what we want to be able to do is to use a chip that was not created by the original manufacturer or to use feedstock attached to a chip in a cartridge where the feedstock was not created by the original manufacturer with that 3D printer."); *id.* at 127:23-128:01 (Siy, Public Knowledge).

[2393] Stratasys Opp'n at 10 (asserting that "circumvention that would allow a 3D printer to process materials whose properties vary intentionally from those for which a system is calibrated[] . . . requires unauthorized modification of copyright protected software").

[2394] *Id.*

[2395] *Id.* at 10-11.

[2396] Tr. at 165:18-24 (May 28, 2015) (Carey, Stratasys) ("The design software is separate from what we do. There are CAD vendors that [] make the design software. We accept all those files."); Stratasys Opp'n at 28 (referencing Autodesk's open source 3D printing software platform).

[2397] *See* Stratasys Opp'n at 11 ("[I]ntellectual property may belong to the manufacturer or to third parties, such as third-party creators of design files provided pursuant to a license.").

According to Stratasys, internal software on its printers converts CAD files into proprietary "CMB" files, which "consist of machine-readable instructions for building a printed part" on a Stratasys printer.[2398] The "motion control and system control software embedded on the printer translate the instructions in the CMB file to cause the hardware to act on the materials in precise ways."[2399] Stratasys claims that "[a] user who wanted to change the behavior of the hardware to work with different materials would need to modify each component of this process, the motion control software, the system control software, and the CMB files."[2400] Finally, Stratasys states that 3D printers may collect "a customer's proprietary or other confidential information," such as customer accessible performance data.[2401]

b. Asserted Noninfringing Uses

Public Knowledge claims that circumventing a chip-based verification system on a 3D printer in order to use third-party feedstock is a "perfectly lawful" noninfringing use and that manufacturers' desire to limit the use of third-party feedstock is "remote" from the proper scope of copyright law.[2402] In addition, Public Knowledge contends that because the software is embedded in the 3D printer and has "no market value independent of the printer itself," 3D printer manufacturers are "unlikely" to be concerned over unauthorized reproduction and distribution of the software separate from the printer it is embedded within.[2403]

Public Knowledge asserts that any necessary reproductions of software would be noninfringing as a fair use under section 107 or under section 117's limitation on exclusive rights for computer programs.[2404] Although Public Knowledge did not directly address the four fair use factors under section 107, it made arguments that indirectly speak to these factors. First, regarding the purpose and character of the use, Public Knowledge claims that the TPMs at issue prevent the use of non-authorized feedstock in 3D printers, but are not intended to protect the copyrighted software itself.[2405] Public

---

[2398] *Id.* Stratasys also creates software that "convert[s] design files into machine readable instructions." *Id.* at 8.

[2399] *Id.* at 11.

[2400] *Id.*

[2401] *Id.* at 22.

[2402] Public Knowledge/LCA Supp. at 6-8. Public Knowledge also argues that Congress would support "treat[ing] machine-embedded software differently than other protected works[,]" pointing to the fact that in section 109, Congress chose to exempt certain computer programs embodied in machines from the general prohibitions on renting, leasing, or lending computer programs. *Id.* at 7; *see also* 17 U.S.C. § 109.

[2403] Public Knowledge/LCA Supp. at 6.

[2404] Tr. at 186:21-23 (May 28, 2015) (Siy, Public Knowledge) ("I think that fair use can cover [printer operating system software] modification."); Public Knowledge Reply at 2 & n.8. One comment also claims that "tinkering" with 3D printers would be a fair use. Digital Right to Repair Class 26 Supp. at 911 (Kenneth Kolbly).

[2405] Public Knowledge 3D Printing Pet. at 3.

Knowledge also notes that interoperability is a recognized purpose under the fair use doctrine.[2406] Second, concerning the nature of the copyrighted work, Public Knowledge states that "[the software] is only useful when paired with the durable good itself,"[2407] suggesting that the software is to a significant degree functional in nature. Third, regarding the amount and substantiality used in relation to the copyrighted work as a whole, Public Knowledge suggests that necessary alterations to use non-authorized feedstock "can vary."[2408] Fourth, addressing the effect of the use upon the potential market for or value of the copyrighted work, Public Knowledge argues there is no real market for the printer software, as it "has no market value independent of the printer itself, and is not marketed independently of the printer."[2409]

Section 117 allows the owner of a computer program to make a copy or adaptation of that work if the new copy or adaptation is created as an "essential step" to use the program with a machine.[2410] Public Knowledge maintains that section 117 allows owners of copies of the printer operating system software to modify that software to use it with the 3D printer.[2411] First, Public Knowledge asserts that the owners of 3D printers also own the copies of the printer operating system software on those printers and that, as owners, they are entitled to exercise their privilege to make copies or adaptations of those programs under section 117.[2412] Second, Public Knowledge contends that any reproductions or modifications made to printer operating system software are essential to utilize third-party feedstock in a 3D printer.[2413] Proponent Michael Weinberg[2414] was not as sanguine on the ownership issue, however; he testified that "especially in the consumer market," there were different degrees of legal sophistication of 3D printer manufacturers and that "it would be highly surprising if you did not see almost every version of copyright license theory applied to software in this space . . . ."[2415]

[2406] *Id.* (citing *Lexmark Int'l, Inc. v. Static Control Components*, 387 F.3d 522 (6th Cir. 2004)).

[2407] Public Knowledge/LCA Supp. at 6.

[2408] Tr. at 132:01 (May 28, 2015) (Siy, Public Knowledge).

[2409] Public Knowledge/LCA Supp. at 6.

[2410] 17 U.S.C. § 117(a)(1).

[2411] Public Knowledge Class 26 Reply at 3.

[2412] *Id.* at 3 n.13.

[2413] Tr. at 143:12-17 (May 28, 2015) (Siy, Public Knowledge) ("[T]he reproductions that might be at issue would be RAM copies made simply in the utilization of the 3D printer itself or any modifications necessary in order to utilize a 3D printer with the new feedstock, and both of these fall within Section 117.").

[2414] At the time of the filing of its petition and supporting comments, Michael Weinberg was employed by Public Knowledge. Weinberg subsequently left Public Knowledge and filed reply comments and testified in his personal capacity. *Id.* at 123:15-20 (Weinberg).

[2415] *Id.* at 148:10-17 (Weinberg).

c. Asserted Adverse Effects

Public Knowledge contends that the inability to circumvent TPMs on 3D printers to use third-party feedstock creates "a significant negative impact on innovation in the 3D printing field, [drives] up costs for consumers, and undermin[es] expectations of ownership around 3D printers."[2416] According to Public Knowledge, manufacturer-approved feedstock costs "three times as much as [feedstock offered by] its third party competitor."[2417] Public Knowledge claims that an exemption would "encourage innovation by protecting and growing the market for innovation in consumables" and points to a general movement towards using diverse and innovative filaments, such as translucent or metal feedstock and even living tissue.[2418] As support, Public Knowledge provides examples of printing living tissues to aid in organ transplants and of a functional 3D-printed boat created out of recycled milk jugs.[2419]

Public Knowledge further states that an exemption would "[r]eaffirm [p]ublic [c]onfidence in [o]wnership" of 3D printers.[2420] It also claims that an exemption would allow consumers and the 3D printing industry to avoid the legal uncertainty experienced in the 2D printing industry before "a landmark court ruling" affirmed consumers' ability to use third-party ink in paper and ink printers.[2421]

Finally, Public Knowledge notes that the existence of TPM-free options offered by some 3D printer manufacturers "does nothing to diminish the importance of this exemption," and that "[a]llowing manufacturers to distort the aftermarket for filament simply because there are other manufacturers in the market would be a misuse of copyright law."[2422] Emphasizing the importance of consumer choice, Weinberg testified that different 3D printers have unique functionalities, and that consumers differentiate between printers by comparing technical or physical properties, which are often patented.[2423]

d. Argument Under Statutory Factors

Reviewing the statutory factors in section 1201(a)(1), Public Knowledge asserts that "the first three factors do not directly apply to this exemption," explaining that "the circumvention of technological measures designed to prevent the use of third party consumables in 3D printers is not the type of harm that Congress was considering when it

[2416] Public Knowledge/LCA Supp. at 8.

[2417] *Id.* at 10.

[2418] *Id.* at 9, 13.

[2419] Public Knowledge 3D Printing Pet. at 4 nn.1-2.

[2420] Public Knowledge/LCA Supp. at 11.

[2421] *See id.* at 10. Public Knowledge does not provide a citation, but presumably is referring to *Lexmark*, 387 F.3d 522.

[2422] Public Knowledge/LCA Supp. at 11.

[2423] Tr. at 182:02-13 (May 28, 2015) (Weinberg).

passed the DMCA."[2424] According to Public Knowledge, the fourth factor, which evaluates the market for copyrighted works, favors granting an exemption because the TPM is not "primarily designed" to protect the operating system software, which is not sold separately from the printer.[2425] Public Knowledge argues that the value of that software "is tied to the value of the printer, and the value of the printer is not connected to the existence or nonexistence of the exemption."[2426] Weinberg also claims that consumers discriminate based on the technical features and capabilities of various 3D printers, without evaluating the copyrighted printer operating system software.[2427]

Public Knowledge contends that the fifth statutory factor, which evaluates such other factors as the Librarian considers appropriate, is the most significant.[2428] Discussing that factor, Public Knowledge argues that an exemption would strengthen property rights,[2429] encourage competition and innovation,[2430] and meet consumer expectations concerning ownership of consumer devices.[2431] Comments received from individual consumers echo this sentiment concerning ownership, with most essentially stating "I own my 3D printer and should be able to use it to print with whatever I want."[2432] These comments also express expectations that 3D printers should be treated the same as 2D printers under the law.[2433]

2. Opposition

Proposed Class 26 is opposed by Stratasys and the Intellectual Property Owners Association ("IPO"). They argue that proponents have failed to make a *prima facie* case

[2424] Public Knowledge/LCA Supp. at 11-12; *see also Lexmark*, 387 F.3d at 551-53. The first three factors consider issues such as "the availability for use of copyrighted works" for general and certain nonprofit purposes and considerations regarding "criticism, comment, news reporting, teaching, scholarship, or research." 17 U.S.C. § 1201(a)(1)(C)(i)-(iii).

[2425] Public Knowledge/LCA Supp. at 12.

[2426] *Id.*

[2427] Tr. at 182:09-13 (May 28, 2015) (Weinberg).

[2428] Public Knowledge/LCA Supp. at 12; 17 U.S.C. § 1201(a)(1)(C)(v).

[2429] Public Knowledge/LCA Supp. at 13 ("Ownership is an important property right, and this exemption would strengthen that right by removing uncertainty surrounding what can and cannot be done with printers.").

[2430] *Id.* (An exemption "would encourage innovation by protecting and growing the market for innovation in consumables.").

[2431] *Id.* at 12 ("Users would be surprised—rightly so—if copyright law prevented them from replacing parts of their noncopyrightable devices simply because the manufacturer included a digital verification chip in its design.").

[2432] *See, e.g.*, Digital Right to Repair Class 26 Supp. at 4 (Aaron Dudek).

[2433] *Id.* at 31 (Adrian Gill) ("I don't need to ask permission from HP if I want to put different ink or paper into my normal printer, and there's no difference."); *id.* at 289 (Christian Moomaw) ("That's like telling me that I can only use paper from certain manufacturers in my printer.").

in support of an exemption and that the balance of statutory factors weighs against their proposal.[2434]

a. Asserted Noninfringing Uses

Opponents maintain that proponents have not documented "distinct, verifiable and measureable impacts . . . actually occurring in the marketplace," but instead only "speculative or insignificant harms."[2435] Stratasys also contends that proponents' proposed uses—using non-manufacturer-approved feedstock or new feedstock materials—do not qualify as noninfringing uses because "[c]ircumvention of a [TPM] that does not control access to a copyright-protected work is beyond the scope of the rulemaking and cannot support an exemption"[2436] and because Public Knowledge "make[s] no argument or comment as to how modifying operating system software or firmware could be a noninfringing use."[2437]

Opponents do not address the fair use factors, with Stratasys maintaining instead that proponents did not even contend that fair use applied.[2438] Stratasys disputed section 117's applicability on the ground that purchasers license rather than own the software in a 3D printer.[2439] Specifically, a Stratasys representative claimed that all of its 3D printers come with a license for the software.[2440] Proponents do not refute this claim.

b. Asserted Adverse Effects

Stratasys believes that proponents' asserted adverse effects are insubstantial because "'[u]ndetermined expectations of ownership,' 'uncertainty,' and 'anxiety about the proper role of copyright' do not constitute the 'distinct, verifiable, and measurable impacts' required to meet the rulemaking standard."[2441] Stratasys claims that evidence of "dissatisfaction [at] not being able to use the material of one's choice in a 3D printer" is

[2434] Stratasys Opp'n at 2; IPO Class 26 Opp'n at 2.

[2435] IPO Class 26 Opp'n at 2 (citing NOI, 79 Fed. Reg. at 55,690); *see also* Stratasys Opp'n at 13 (arguing that proponents "cannot obtain an exemption from liability for undefined acts of circumvention" and that proponents' comments in support "do not provide a sufficient record on which to base an exemption").

[2436] Stratasys Opp'n at 13.

[2437] *Id.* at 14.

[2438] *Id.* ("Petitioners have not offered any argument that fair use or another statutory exception operates to render such activity non-infringing."). Stratasys' representative did not respond to proponents' assertions at the hearing that fair use applied to this class.

[2439] Perhaps because proponents asserted that the proposed uses were noninfringing under section 117 only in reply comments, Stratasys disputed this position during the public hearing as opposed to in written comments. *But see id.* at 13 n.58 (noting that the 2010 Rulemaking found that cellphone unlocking was likely noninfringing under section 117).

[2440] Tr. at 164:09-13 (May 28, 2015) (Carey, Stratasys; Charlesworth, USCO).

[2441] Stratasys Opp'n at 15 (citing 2010 Final Rule, 75 Fed. Reg. at 45,833).

"of minimal probative value because [proponents] do not link such dissatisfaction regarding this constraint to TPMs."[2442]

Stratasys also disputes that TPMs discourage innovation in 3D printing, alleging that closed systems allow for greater revenue from materials sales to support research and development into new materials and that independent developers are free to use open systems for experimentation.[2443] Stratasys points to the large amount of investment made in 3D printing technologies, noting that the development of feedstock materials is Stratasys' "greatest area of investment."[2444] Stratasys notes that proponents "do not point to one instance of an independent materials producer hampered by TPMs."[2445] Stratasys adds that engineering constraints necessarily limit use of different materials, as feedstock materials require fine-tuning of temperatures, print nozzles can only process feedstock of a particular diameter, and extruders cannot tolerate materials that are abrasive or physically or chemically different from manufacturer-approved feedstock.[2446] Finally, Stratasys claims that use of non-manufacturer-approved feedstock to save cost "is a matter of convenience and preference" and not "the type of adverse impact[] the rulemaking is intended to address."[2447]

c. Argument Under Statutory Factors

Stratasys argues that the statutory factors weigh against granting an exemption, although it agrees with proponents that factors two and three are of "limited applicability" to this proposed class.[2448] Stratasys asserts that the first factor, "the availability for use of copyrighted works," weighs against granting an exception because the TPMs at issue "increase[] the availability in the marketplace of particular kinds of 3D printing systems."[2449] It also indicates that TPMs on the operating system software of the 3D printer protect other proprietary material stored on the printer, namely, "design software, design files, and proprietary data collected during the printing process, such as customer-accessible performance data," although it does not provide details.[2450] Notably, Stratasys does not appear to contend that the chip-based TPMs used to exclude non-manufacturer-approved feedstock are employed to protect this material.

Looking to the fourth factor, Stratasys claims that an exemption would harm the market for copyrighted works "in at least three ways: (1) it would threaten the value of a

[2442] *Id.* at 15-16.

[2443] *Id.* at 16; Tr. at 181:14-20 (May 28, 2015) (Carey, Stratasys).

[2444] Tr. at 181:17-20 (May 28, 2015) (Carey, Stratasys).

[2445] Stratasys Opp'n at 17.

[2446] *Id.* at 16.

[2447] *Id.* at 18.

[2448] *Id.* at 23.

[2449] *Id.* at 21-22.

[2450] *Id.* at 22; *see also* IPO Opp'n at 4.

manufacturer's 3D printers; (2) it would undermine security protections for intellectual property and confidential information embedded on printers; and (3) it would undermine growth in the overall market for 3D printers and 3D printed objects by placing at risk technological advances enabled by secure, fully-integrated 3D printing systems."[2451] Stratasys argues that some companies are starting to offer stand-alone 3D printer operating system software, though the example it cites is of an open source program.[2452] Stratasys draws an analogy to the 2012 Rulemaking, which it states protected embedded software in video game consoles, and thus protected both the console operating system code as a secure distribution platform, and also protected the video games themselves.[2453] Stratasys argues that denying an exemption in this case would similarly protect the value of 3D printers as "secure platforms for the distribution of proprietary design and modeling software and design files," as well as the intellectual property embedded in those printers.[2454]

Under the fifth factor, Stratasys offers public policy arguments relating to economic, quality control, and branding concerns. Stratasys claims that "[p]rinter manufacturers rely on anticipated revenue streams from the sale of materials in order to make printers available at attractive prices" to reach more consumers.[2455] In short, it argues that an exception would threaten manufacturers' ability to engage in "metering,"[2456] which allows manufacturers to "set the price of the printer lower than they would otherwise, in order to sell more printers and increase their profits from selling materials."[2457]

Stratasys asks the Register to consider that circumvention could decrease consumer benefits by bypassing "smart" feedback cartridge microchip technology that can "measure the amount of material remaining in a cartridge and [] notify the printer operator when replacement or service is required."[2458] Stratasys claims that this performance-monitoring technology is vital for "effective rapid prototyping" and "direct digital manufacturing, especially for sensitive applications such as medical implants and aerospace parts."[2459] Opponents emphasize the importance of using authorized materials

[2451] Stratasys Opp'n at 23.

[2452] *Id.* at 28 (citing Rakesh Sharma, *The Autodesk 3D Printer: A Calculated Bet*, FORBES (Mar. 23, 2014), http://www.forbes.com/sites/rakeshsharma/2014/05/23/the-autodesk-3d-printer-a-calculated-bet).

[2453] *Id.* at 23.

[2454] *Id.* at 23-24 (claiming an exemption would "negatively affect a manufacturer's reputation and the image of the manufacturer's systems in the marketplace" by printing substandard objects made with non-manufacturer-approved feedstock and would hinder the ability to collect service performance data).

[2455] *Id.* at 27.

[2456] Metering is a type of tying that "uses demand for the tied product to measure expected demand for the tying product." Thomas A. Lambert, *Appropriate Liability Rules for Tying and Bundled Discounting*, 72 OHIO ST. L.J. 909, 917 (2011).

[2457] Stratasys Opp'n at Exhibit A at 11.

[2458] *Id.* at 28.

[2459] *Id.*

for 3D printing, stating that "[c]omposite materials have been demonstrated to damage the [printer's] extruder."[2460] In essence, opponents argue that some materials should never be used in certain 3D printers, because the mechanical properties of the printer are not suited to such use.

Even where use of alternate materials is possible, Stratasys is concerned that printing using non-optimized feedstock "may result in poorer quality printed objects or damage to the printer, both of which adversely affect the printer manufacturer's reputation."[2461] Stratasys argues that certain industrial applications require a high degree of precision, for example, "medical implants, aerospace parts, or consumer goods subject to strict safety standards," and some printer materials are engineered to be "food-safe, colorful, flexible, or durable, and to resist flame, smoke, high-temperatures, fatigue, and mechanical stress."[2462] It further notes that its industrial customers test 3D printers to ensure quality to make sure they are fit for a particular use,[2463] and that federal regulations may impose certification or manufacturing requirements that apply to 3D-printed goods.[2464] Stratasys raises the serious concern that someone who is printing products for such regulated uses might break a TPM to use an "inferior material" to print parts that could endanger a downstream user.[2465] Although these concerns appear directed towards industrial operations, Stratasys believes that the exemption should be denied for both consumer and commercial uses, cautioning that "[t]here is a spectrum of 'prosumers' (*i.e.*, 'professional consumers') and crowd-sourced communities [that] commercialize their use of 3D printers to varying degrees."[2466]

3. Discussion

Public Knowledge seeks a broad exemption comprising every 3D printer using TPMs, and encompassing those sold for both consumer and industrial uses. As an initial matter, it appears that the technological properties of 3D printers, including the use of TPMs,[2467] the relative complexity of those TPMs,[2468] and the technological features of 3D printers,[2469] vary greatly. The record suggests that, depending on the software

[2460] *Id.* at 29.

[2461] *Id.*

[2462] *Id.* at 5.

[2463] *Id.* at Exhibit A at 6 ("Stratasys' industrial customers, seeking to use 3D printing to create tools or parts, typically ask to see and test benchmarks (examples) before purchasing a printing system, in order to ensure that the quality and the specifications of the printed model meet their needs.").

[2464] Tr. at 154:16-23, 156:13-158:09 (May 28, 2015) (Charlesworth, USCO; Carey, Stratasys) (citing Federal Aviation Administration, Food and Drug Administration ("FDA"), and general Federal Acquisition Regulations).

[2465] *Id.* at 159:16-160:16 (Cheney, NTIA; Carey, Stratasys).

[2466] Stratasys Opp'n at 3.

[2467] Public Knowledge/LCA Supp. at 5-6; Stratasys Opp'n at 10.

[2468] Tr. at 134:19-136:08 (May 28, 2015) (Weinberg; Charlesworth, USCO).

[2469] *See id.* at 182:02-13 (Weinberg); *see also* Stratasys Opp'n at 3.

implementation on the printer, users may or may not need to copy the printer operating system software to make the modifications required to use third-party feedstock.[2470] Stratasys listed over 250 companies producing consumer 3D printers and 33 companies producing industrial 3D printers, including a number of non-TPM-protected printers, with wide-ranging capabilities, prices and feedstock options.[2471] Proponents focus their evidence on chip-based verification methods, so that is the Register's focus as well in considering the proposed exemption.[2472]

At the outset, the Register notes that both proponents and opponents appear to acknowledge that in some cases, forcing a 3D printer to accept third-party feedstock may not run afoul of section 1201(a)(1). Although the record lacks specifics, it appears that in some cases, the necessary alteration may not involve a copyrighted work.[2473] Additionally, there is some support in case law for the conclusion that where a chip on a feedstock cartridge contains a simple code, but the software is otherwise freely readable after purchasing the printer, the code may not effectively control access to a work.[2474] In such cases an exemption would be unnecessary under section 1201(a)(1). But it appears there are other cases where a consumer wishing to use third-party feedstock in a 3D printer would need to engage in circumvention of a TPM protecting a copyrightable work, for example, when more complex code must be modified so the printer can handle alternative feedstock. It is therefore appropriate to proceed with the analysis.

a. Noninfringing Uses

Although their legal analysis is somewhat limited,[2475] the Register concludes that Class 26 proponents have sufficiently established that the copying and modification of printer software to accept alternative printing materials is likely to be a noninfringing use.

[2470] Tr. at 141:15-22 (May 28, 2015) (Charlesworth, USCO; Weinberg).

[2471] Stratasys Opp'n at Exhibit A at 4 (citing WOHLERS REPORT at 59, 99); *see also id.* at 19-21.

[2472] Tr. at 134:19-135:04 (May 28, 2015) (Weinberg).

[2473] *See id.* at 127:03-12 (Siy, Public Knowledge); Stratasys Opp'n at 14 ("To the extent that Petitioners argue that certain methods of chip-based circumvention do not violate the DMCA because the chip is not controlling access to a copyright-protected work, then . . . an exemption for such circumvention is not within the scope of the rulemaking.").

[2474] *See Lexmark*, 387 F.3d at 547 ("Just as one would not say that a lock on the back door of a house 'controls access' to a house whose front door does not contain a lock and just as one would not say that a lock on any door of a house 'controls access' to the house after its purchaser receives the key to the lock, it does not make sense to say that this provision of the DMCA applies to otherwise-readily-accessible copyrighted works. Add to this the fact that the DMCA not only requires the technological measure to 'control access' but also requires the measure to control that access 'effectively,' and it seems clear that this provision does not naturally extend to a technological measure that restricts one form of access but leaves another route wide open." (citation omitted)). Courts may also disfavor use of printer verification chips as TPMs if their primary purpose is to prevent use of consumables in consumer goods. *See id.* at 553 (Merritt, J., concurring).

[2475] Tr. at 186:21-23 (May 28, 2015) (Siy, Public Knowledge) ("I think that fair use can cover [printer operating system software] modification.").

The Register observes that the question here appears somewhat analogous to that addressed by the Sixth Circuit in *Lexmark International, Inc. v. Static Control Components, Inc.*, in which the court considered whether a third party manufacturer of toner cartridges violated the Copyright Act when it reverse-engineered and then reproduced a manufacturers' verification chip on toner cartridges. There, as here, the third-party circumvented a TPM so that non-manufacturer-approved cartridges could be used with a printer.[2476] In *Lexmark*, the Sixth Circuit discussed policy issues also relevant to this class, concluding that Congress did not intend for the DMCA to "create monopolies of manufactured goods."[2477] The court further suggested that technological measures that protect access to creative works, such as video games or DVDs, were at the core of what the DMCA was intended to protect, rather than the functional aspects of printer operating system programs.[2478]

Turning more specifically to the question of fair use, regarding the first factor, the purpose and character of the use, the Register notes that interoperability is recognized as a favored purpose under the law.[2479] The record shows that in many cases, third-party feedstock cannot be used without altering the printer operating system software.[2480] This factor therefore favors proponents.[2481]

[2476] *Lexmark*, 387 F.3d at 528-529.

[2477] *Id.* at 551 (Merritt, J., concurring); *see also id*. at 553 (Feikens, J., concurring in part and dissenting in part) ("We agree that the [DMCA] was not intended by Congress to be used to create a monopoly in the secondary markets for parts or components of products that consumers have already purchased.").

[2478] *Id.* at 548.

[2479] *See, e.g., id.* at 544, 545-546 (discussing interoperability and noting that, under the first factor, the defendant did not copy the program at issue "for its commercial value *as a copyrighted work*" (emphasis in original)); *see also Sega Enters. Ltd. v. Accolade, Inc*., 977 F.2d 1510, 1522-23 (9th Cir. 1992) (under the first statutory factor, copying of software for "identification of the functional requirements for . . . compatibility" was a public benefit, did not harm the original work's commercial value, and favored a finding of fair use).

[2480] Stratasys Opp'n at Exhibit A at 5 ("New materials . . . require tuning the system parameters (controlled by software) to the material's properties . . . .").

[2481] Congress recognized the importance of compatibility in the DMCA by including a statutory exemption to the prohibition on circumvention for certain reverse engineering activities. *See* 17 U.S.C. § 1201(f); *see also* 144 CONG. REC. E2138 (daily ed. Oct. 13, 1998) (statement of Rep. Bliley) (stating that "section 1201 should not inhibit interoperability of devices 'in the consumer electronics environment'"). But, for the reasons that follow, section 1201(f) may not protect the activities at issue here and so does not obviate the need for an exemption under section 1201(a)(1). Section 1201(f) requires that the circumvention be performed by the person who "identif[ies] and analyz[es] those elements of the [software] program that are necessary to achieve interoperability." 17 U.S.C. § 1201(f)(1). As the Register concluded in 2010 when considering an exemption to allow jailbreaking of smartphones, and again in 2012 when considering video game consoles, when an exemption is sought to permit anyone to circumvent a TPM—and "not just those who [perform] 'identification and analysis' of programmatic elements"—it creates "significant doubt" as to whether section 1201(f) would apply. 2012 Recommendation at 45 n.212 (citing 2010 Recommendation at 94-95 & n.318).

Concerning the second factor, the nature of the work, the Register notes that proponents wish to access the work not for its creative appeal, but because the work is useful in printing 3D objects. In other words, the work to be accessed is functional in nature. This factor thus favors proponents.

The third factor considers the amount and substantiality used in relation to the copyrighted work as a whole, but there was very little record of how much the printer operating system software would need to be changed to use third-party feedstock—only that it could "vary." [2482] This factor thus favors neither party.

Factor four, which is highly contested, considers "the effect of the use on the potential market for or value of the copyrighted work."[2483] Public Knowledge suggests that the market at issue is very narrow, consisting of only the printer operating system software, which "has no market value independent of the printer itself, and is not marketed independently of the printer."[2484] Stratasys points to the large market value of the overall 3D printer industry.[2485] In essence, opponents urge the Office to take a broader view of the effects of circumvention on the market as a whole.

Here, the Sixth Circuit's *Lexmark* decision is again instructive. Although that case was ultimately decided on other grounds, in conducting a fair use analysis, the court determined that the proper focus was on the market for the copyrighted work (the printer operating system software) and not the market for the consumable (the toner cartridges).[2486] Based on the record submitted here, there does not appear to be a market for printer operating system programs separate from the 3D printers themselves, or a quantifiable way to apportion the value of the 3D printer attributable to the software features. Although opponents suggest that feedstock sales by manufacturers may subsidize the retail cost of printers, there was no evidence presented to establish that the use of unauthorized feedstock would substantially undermine printer sales. Moreover, as discussed below, manufacturers' pricing policies are not the focus of copyright law. For these reasons, the fourth fair use factor does not weigh against proponents.

As three of the four fair use factors favor proponents, and one is neutral, the Register concludes that necessary copying and alteration of 3D printer software to accommodate alternative feedstock likely constitute fair use of such a work.

The Register further concludes that the overall record supports proponents' claim that modifying software to permit use of non-manufacturer-approved feedstock may also

[2482] Tr. at 132:01 (May 28, 2015) (Siy, Public Knowledge) (amount "can vary"); *id.* at 188:09 (Carey, Stratasys) (not aware of how much of a change in software would be needed).

[2483] *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 590 (1994) (quoting 17 U.S.C. § 107(4)).

[2484] Public Knowledge/LCA Supp. at 6.

[2485] Stratasys Opp'n at 25-26.

[2486] *Lexmark*, 387 F.3d at 544-45.

be a non-infringing use under section 117, at least in some cases.[2487] Section 117(a) allows the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that program created "as an essential step in the utilization of the computer program in conjunction with a machine and that . . . is used in no other manner."[2488] The limited factual record[2489] makes it difficult to determine whether purchasers of 3D printers are likely to qualify as "owners" of the accompanying software under section 117. Proponents raised the issue only in reply comments and submitted no sales terms or other evidence to support their contention that consumers own the software. At the hearing, Weinberg acknowledged that at least some 3D printers are likely sold with terms purporting to license the printer's operating system software, but contended that in many cases, there are no terms.[2490] For its part, Stratasys attests that its printer operating system software is subject to an explicit license, but it did not represent that this was true of the industry generally.[2491]

Based on this limited information, it appears likely that in at least some cases, purchasers of 3D printers may be owners for purposes of section 117. The Register has previously reviewed the relevant case law governing the determination of ownership of a software copy for purposes of section 117 when formal title is lacking and/or a license or agreement imposes restrictions on the use of the computer program and concluded that the state of the law is unclear.[2492] While *Vernor v. Autodesk, Inc.*[2493] and *Krause v. Titleserv, Inc.*[2494]—the two leading precedents in this area—provide "useful guideposts," they are "controlling precedent in only two circuits and are inconsistent in their approach."[2495]

In *Krause*, the Second Circuit held that formal title was not necessary to demonstrate ownership under section 117, but instructed courts to look to a range of

---

[2487] Public Knowledge Class 26 Reply at 3 ("17 U.S.C. § 117 facilitates the modification of software by owners of a copy of the software [who use] the software . . . with a machine (the printer) [by providing that use] is expressly not an infringement."); Tr. at 143:12-144:14 (Siy, Public Knowledge; Charlesworth, USCO) (referencing section 117).

[2488] 17 U.S.C. § 117(a).

[2489] The Register notes that analysis of this class generally was hampered by a limited factual record—especially as presented by proponents—and reminds the parties that "[i]n addressing factual matters, commenters should be aware that the Register favors specific, 'real-world' examples supported by evidence over speculative, hypothetical observations." NPRM, 79 Fed. Reg. at 73,857.

[2490] Tr. at 148:09-19 (May 28, 2015) (Weinberg).

[2491] *Id.* at 164:06-25 (Charlesworth, USCO; Carey, Stratasys) (asserting that Stratasys' software is subject to a license in every case).

[2492] *See* 2010 Recommendation at 90 (stating that "the law relating to who is the owner of a copy of a computer program under Section 117 is in flux"); *see also id.* at 129, 132; 2012 Recommendation at 92 ("The Register concludes that the state of the law remains unclear.").

[2493] 621 F.3d 1102 (9th Cir. 2010).

[2494] 402 F.3d 119 (2d Cir. 2005).

[2495] 2012 Recommendation at 92.

factors to determine "whether the party exercises sufficient incidents of ownership over a copy of the program to be sensibly considered the owner of the copy."[2496] In *Vernor*, the Ninth Circuit held that "a software user is a licensee rather than an owner of a copy where the copyright owner (1) specifies that the user is granted a license; (2) significantly restricts the user's ability to transfer the software; and (3) imposes notable use restrictions."[2497]

In this proceeding, other than possible updating or patching of software,[2498] there is little evidence that printer manufacturers exert continuing control over printer software, suggesting that some purchasers of 3D printers may qualify under existing case law as "owners" under section 117. That said, the Register recognizes that more sophisticated 3D printers—for example, those used in industrial enterprises—may involve more substantial ongoing relationships between the printer manufacturer and the end user, and it is possible that the software in such printers is subject to a license.[2499]

Users of 3D printer operating system software who do meet the ownership requirement of section 117 must also show that alteration of the software is essential to operate the software in connection with the printer.[2500] The record seems undisputed that to successfully operate some TPM-protected 3D printers with third-party materials, it may be necessary to alter the operating system software.[2501] Based on the record submitted, it therefore appears likely that some activities in which proponents seek to engage could qualify as noninfringing uses under section 117.

b. Adverse Effects

Public Knowledge claims that the lack of an exemption increases consumer costs and has a significant negative impact on 3D printing innovation.[2502] At the same time,

---

[2496] *Krause*, 402 F.3d at 124. These factors include: (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. *Id.*

[2497] *Vernor*, 621 F.3d at 1111.

[2498] Tr. at 166:08-09 (May 28, 2015) (Carey, Stratasys).

[2499] *See* Stratasys Opp'n at Exhibit A at 6 ("Industry-wide, high-end 3D printing systems more commonly employ software verification than desktop (entry-level) printing systems, and (as with Statasys' high-end systems) customers of high-end printing systems typically purchase material from the printer manufacturer.").

[2500] 17 U.S.C. § 117(a).

[2501] Stratasys Opp'n at Exhibit A at 5 ("New materials . . . require tuning the system parameters (controlled by software) to the material's properties . . . .").

[2502] Public Knowledge/LCA Supp. at 8. Public Knowledge also claims that granting an exemption would "[r]eaffirm [p]ublic [c]onfidence in [o]wnership," but has provided little by which the Register may evaluate this claim. *Id.* at 11.

the record reflects that there is a good selection of non-TPM-protected printers on the market that do not restrict feedstock, albeit with varying capabilities.

The Register finds that proponents have demonstrated that the use of TPMs to restrict the use of third-party feedstock may inhibit some consumers' ability to make noninfringing uses of 3D printer software. The Register notes that the mere fact that manufacturer-approved feedstock may cost more is not an adverse effect stemming from the prohibition on circumvention. But consumers may have reasons beyond cost to use alternative materials in a 3D printer, and a TPM may prevent that type of interoperability. Moreover, while there may be a variety of 3D printers in the market, including some without TPMs, proponents provided evidence that certain printers that are protected by TPMs have unique and desirable functions that may not be available in non-TPM-protected printers.[2503] Further, while opponents may well be correct that the technical constraints of certain printer models may present significant challenges to some of the proposed uses,[2504] it does not change the fact that a particular printer may be unusable with alternative materials absent circumvention.[2505]

For these reasons, the Register believes that proponents have demonstrated that the inability to circumvent TPMs in some 3D printers is likely to have an adverse impact on noninfringing activities in the upcoming three-year period.

c. Statutory Factors

While the five statutory factors do not uniformly favor proponents, for the reasons discussed below, the Register finds that overall, the statutory factors favor granting an exemption. An exemption will serve to increase the ability of consumers to create new works using innovative methods and appears unlikely to materially adversely impact the market for copyrighted 3D printer software.

With respect to the first factor, the availability for use of copyrighted works, the Register first considers whether an exemption is likely to affect the availability of copyrighted printer operating software. The current record does not demonstrate that an exemption would threaten the availability of such software, or, indeed, that a viable market for this type of software exists separate from the printers themselves. Further, altering such software for purposes of interoperability in this case is likely a fair use or allowed under section 117.

[2503] *See* Tr. at 183:03-05 (May 28, 2015) (Weinberg) (explaining that some functional processes of 3D printers are patented, and are only available with a specific manufacturer); *see also* Stratasys Opp'n at 3 ("3D printer users benefit from having a variety of systems in the market so they can choose the system suited to their intended use. . . . [D]ifferent technological approaches confer different advantages").

[2504] Stratasys Opp'n at 16.

[2505] The Register notes that users modifying a 3D printer to circumvent a TPM may be breaking the printer's warranty. Tr. at 168:12-17 (May 28, 2015) (Charlesworth, USCO; Carey, Stratasys); *id.* at 138:02-03 (Weinberg).

Nor is there evidence that granting the exemption will adversely affect the availability of copyrighted works besides the printer software. To be sure, Stratasys claims that 3D printers may contain other proprietary matter besides the software that is used to operate the 3D printer—design software, design files, and proprietary customer data.[2506] According to Stratasys, the TPMs on the operating system software for the 3D printer also protect access to this material, and accordingly it urges the Register to reject the proposed exemption for the same reasons she previously rejected an exemption for jailbreaking of video game consoles, where TPMs protect both the game console firmware and the games that are played on those consoles.[2507] But unlike in the case of video game consoles, there is no evidence in the current record that design software developers or persons creating 3D designs rely on 3D printer TPMs to provide a secure method of distribution for their copyrighted works. Nor is there any evidence that circumventing TPMs would lead to piracy of these proprietary materials. In contrast, in 2012, the record showed that video game consoles were designed to operate as secure distribution platforms for creative works and that TPMs on such consoles were heavily relied on as part of an integrated protection system by all major console video game manufacturers. There, opponents documented that circumvention of consoles directly leads to piracy of copyrighted expressive works; that is, the video games themselves.[2508] In any event, proponents are not seeking access to any design software, design files, or proprietary data, and so any potential exemption can thus be limited solely to circumvention for the use of non-manufacturer-approved feedstock.

Factors two and three, concerning the availability for use of works for nonprofit archival, preservation, and educational purposes and the impact that the prohibition on circumvention has on criticism, comment, news reporting, teaching, scholarship, or research, respectively, do not appear to be germane to this class.

Evaluating the fourth factor, the effect of circumvention on the market for or value of copyrighted works, the Register finds that there is currently no independent

[2506] The record does not reveal the precise nature of the proprietary data that are held on a 3D printer. Stratasys states, without elaboration, that these data include "customer-accessible performance data that may contain a customers' [sic] proprietary or other confidential information." Stratasys Opp'n at 22. To the extent the proprietary data are the customer's *own* data, Stratasys' point is obscure, since it would be the customer (as the owner of the 3D printer) who is engaging in circumvention. Furthermore, the record suggests that design software is often installed on a separate computer, not the 3D printer, and is typically owned by third parties and perhaps licensed to users. Tr. at 165:18-24 (May 28, 2015) (Carey, Stratasys) ("The design software is separate from what we do. There are CAD vendors that . . . make the design software. We accept all those files."). At the same time, neither Public Knowledge nor any other party challenges Stratasys' claim that 3D printers can include both design software and proprietary data. Accordingly, the Register accepts Stratasys' assertion.

[2507] *See* 2012 Recommendation at 47-48.

[2508] *Id.* at 32-36.

market for 3D printer operating software.[2509] Moreover, opponents have not shown how allowing an exemption is likely to diminish the value of a 3D printer's copyrighted software. Opponents again suggest the Register should evaluate 3D printer TPMs in the same manner as TPMs on video game consoles and deny an exemption because, like consoles, the printers operate as secure distribution platforms for other creative works.[2510] As discussed above, there is not enough evidence in the record to support this assertion.

The fifth statutory consideration, which evaluates "such other factors as the Librarian considers appropriate," allows the Librarian to evaluate additional pertinent concerns that might otherwise go unaddressed. Stratasys urges that many 3D printer manufacturers market their products by selling printers for a lower price, while making up for that discount with the sale of manufacturer-distributed feedstock.[2511] Opponents worry that an exemption permitting circumvention might undermine this business practice. While this is certainly a reasonable concern for those in the 3D printing business, it is considerably removed from section 1201(a)(1)'s goal of facilitating and protecting the availability of creative works[2512] and is thus not a basis to deny the exemption.[2513]

Finally, opponents point to regulatory and safety concerns that might arise if an exemption were granted. The record indicates that 3D printing processes are used to produce medical implants, aerospace parts, and consumer goods, which are all subject to strict safety standards.[2514] It is reasonable to suspect that if these types of items were manufactured using alternative materials or with altered printer software, the resulting goods might not comply with the applicable standards. Indeed, some printers of industrial objects are subjected to rigorous testing to certify that their 3D printed products meet industry standards[2515] or are compliant with applicable regulations.[2516]

[2509] Although Stratasys contends that companies are starting to offer stand-alone 3D printing software, the only example provided was of an open source platform. Stratasys Opp'n at 28 (referencing Autodesk's open source 3D printing software platform).

[2510] IPO Opp'n at 4; Stratasys Opp'n at 22.

[2511] Stratasys Opp'n at 27.

[2512] Public Knowledge Class 26 Reply at 2; *see also Lexmark*, 387 F.3d at 549 ("Nowhere in its deliberations over the DMCA did Congress express an interest in creating liability for the circumvention of technological measures designed to prevent consumers from using consumers goods while leaving the copyrightable content of a work unprotected."); *id.* at 551 (Merritt, J., concurring) (stating that "companies like Lexmark cannot use the DMCA in conjunction with copyright law to create monopolies of manufactured goods"); *id.* at 553 (Feikens, J., concurring in part and dissenting in part) ("We agree that the [DMCA] was not intended by Congress to be used to create a monopoly in the secondary markets for parts or components of products that consumers have already purchased.").

[2513] Opponents' additional business-related concerns of a negative impact on the collection of service performance data and reputational harm were also unpersuasive.

[2514] Stratasys Opp'n at 5.

[2515] *Id.* at Exhibit A at 6.

Notably, FDA reinforced this concern in a letter to the Office, explaining that an exemption for this class might create unintended public health and safety risks in relation to medical devices produced using 3D printers.[2517] FDA explained that "manufacturers who utilize 3D printing to ultimately manufacture medical devices need to ensure that their products are safe and effective for their intended use."[2518] For instance, according to FDA, "if a 3D printed medical device is intended for insertion into the body, then the manufacturer under FDA regulations would have to demonstrate that the products are safe and effective for that intended use."[2519]

These safety and regulatory concerns are not copyright-related, but are sufficiently weighty to merit consideration in drafting an exemption. The parties agree that an exemption that attempted to draw a line between noncommercial versus commercial or industrial uses of 3D printers would be difficult in practice.[2520] Because it is clear, however, that the initial proposal was motivated largely by noncommercial, consumer uses,[2521] as set forth below, the Register finds that it is appropriate to limit the exemption to exclude uses that may be subject to regulation or certification.

4. NTIA Comments

NTIA believes that "an exemption [in this class] would benefit consumers and the industry by fueling innovation of new feedstocks and reducing costs of feedstock for consumers."[2522] NTIA notes that in some cases, "it is unclear whether one needs to circumvent a TPM that controls access to a copyrighted work," but in other cases, it appears likely that a copyrighted work is at issue.[2523] NTIA therefore supports an exemption to alleviate "consumer uncertainty regarding the permissibility of circumvention for interoperability of feedstock."[2524] In NTIA's view, the *Lexmark* case also "suggests that copying or modifying a copyrightable program on a 3D printer to enable interoperability with third party feedstock may be seen as fair use."[2525] While

---

[2516] Tr. at 154:12-23, 156:13-157:02 (May 28, 2015) (Charlesworth, USCO; Carey, Stratasys) (citing Federal Aviation Administration, FDA, and general Federal Acquisition Regulations).

[2517] *See* Letter from Bakul Patel, Assoc. Dir. for Digital Health, Ctr. for Devices and Radiological Health, FDA, to Jacqueline C. Charlesworth, Gen. Counsel and Assoc. Register of Copyrights, USCO, at 4 (Aug. 18, 2015).

[2518] *Id.*

[2519] *Id.*

[2520] Public Knowledge Class 26 Post-Hearing Resp. at 1-3; Stratasys Post-Hearing Resp. at 1-3.

[2521] Tr. at 137:19-23 (May 28, 2015) (Weinberg) ("[W]hile this was originally motivated by focus on consumer use, I don't think there is any reason to exclude manufacturing or more sophisticated commercial players.").

[2522] NTIA Letter at 89.

[2523] *Id.*

[2524] *Id.* at 90.

[2525] *Id.* at 91-92 (citing *Lexmark*, 387 F.3d at 549).

acknowledging manufacturer concerns that an exemption could facilitate the introduction of inferior materials into supply chains, NTIA "is troubled by the growing misuse of the DMCA to serve non-copyright interests" and states that "Section 1201 is a poor fit to ensure quality control in [] manufacturing."[2526]

Noting that "manufacturers may use low end or consumer-oriented machines during different parts of the design process," NTIA supports an exemption that "does not distinguish between commercial, noncommercial, or consumer uses of a 3D printer." [2527] Further, it supports a "broad exemption that does not distinguish between technical specifications of TPMs."[2528]

As explained below, the Register finds that the record supports granting an exemption, but recommends that it is tailored to the types of consumer-oriented uses introduced in the record. The record supports excluding circumvention on printers used to produce goods subject to legal or regulatory oversight or related certification processes, to balance the supply chain concerns that NTIA recognizes.

5. Conclusion and Recommendation

The Register concludes that proponents have established that TPMs constrain the types of feedstock that can be used in 3D printers and that this is likely to adversely affect noninfringing uses of the software that controls that functionality. The Register further finds that in some cases the 3D printer operating system software must be altered to print 3D objects using non-manufacturer-approved feedstock. Nonetheless, the record, which focuses on consumer uses, points to a more narrowly defined class than originally suggested. Consistent with past rulemakings, the Register will tailor the proposed recommended exemption to reflect the record evidence.[2529] To begin with, because the record submitted by proponents was limited to 3D printers that employ microchip-based verification systems, the recommended exemption will be tied to 3D printer models that require circumvention of this type of TPM.

Significantly, the Register does not recommend extending an exemption to circumstances where the use of third-party feedstock could cause the resulting 3D-printed object to fail legal requirements or regulatory mandates, including safety certification criteria or other similar standards. Opponent Stratasys raised legitimate concerns regarding the production of regulated products using non-approved feedstock that could then be introduced into the stream of commerce, and FDA noted specific concerns about the use of 3D printers to manufacture medical devices that would be used by patients. At

[2526] *Id.* at 90.

[2527] *Id.* at 91.

[2528] *Id.*

[2529] 2010 Recommendation at 16 (explaining that "the records in [the 2010] and prior rulemaking proceedings have demonstrated that in many cases, [an initial] subset of a category of works should be further tailored in accordance with the evidence in the record").

the same time, as explained above, proponents' case did not focus on these types of uses. Instead, proponents highlighted consumer and experimental uses of 3D printers.[2530] While the parties agree that it may be difficult to demarcate the line between commercial and noncommercial uses of 3D printers, the standards that govern the resulting products are more definitely defined. Users should be free to tinker with their 3D printers, but without putting those further down the stream of commerce at risk.

Finally, in reflection of the record, the recommended exemption is limited to circumvention for the purpose of using alternate feedstock; it does not encompass circumvention for the purpose of accessing design software, design files, or proprietary data.

In keeping with the Register's findings based on the record before her, the Register recommends that the Librarian designate the following class:

> **Computer programs that operate 3D printers that employ microchip-reliant technological measures to limit the use of feedstock, when circumvention is accomplished solely for the purpose of using alternative feedstock and not for the purpose of accessing design software, design files or proprietary data; provided, however, that the exemption shall not extend to any computer program on a 3D printer that produces goods or materials for use in commerce the physical production of which is subject to legal or regulatory oversight or a related certification process, or where the circumvention is otherwise unlawful.**

[2530] *See* NTIA Letter at 91; Tr. at 137:19-23 (May 28, 2015) (Weinberg) (conceding that the proposed exemption was "originally motivated by focus on consumer use").

N. Proposed Class 27B: Networked Medical Devices – Patient Data

1. Proposal

Many modern implanted medical devices, such as pacemakers, implantable cardioverter defibrillators ("ICDs"), insulin pumps, and continuous glucose monitors, measure and record data about physiological developments taking place within the body, and communicate that data wirelessly to equipment maintained at hospitals or doctors' offices, or to corresponding personal monitoring systems. Some personal monitoring systems, in turn, transmit data to a monitoring company and ultimately to the patient's physician. Increasingly, these transmissions of data are protected by TPMs, including encryption schemes. Proponents are requesting an exemption that would allow a patient, or persons acting on behalf of the patient, to circumvent TPMs on these transmissions so that the patient is able to access the data generated by his or her own implanted medical device and any corresponding personal monitoring system, without the need to visit a hospital or doctor's office.

Proponent Medical Device Research Coalition ("MDRC") filed a petition seeking an exemption that covered two proposed uses: (1) allowing patients to access the data generated by their medical devices and any corresponding monitoring systems, and (2) allowing research into software flaws that adversely affect the safety, security and efficacy of medical devices.[2531] The Office set forth the following class in the NPRM:

> Proposed Class 27: The proposed class would allow circumvention of TPMs protecting computer programs in medical devices designed for attachment to or implantation in patients and in their corresponding monitoring devices, as well as the outputs generated through those programs. As proposed, the exemption would be limited to cases where circumvention is at the direction of a patient seeking access to information generated by his or her own device, or at the direction of those conducting research into the safety, security, and effectiveness of such devices. The proposal would cover devices such as pacemakers, implantable cardioverter defibrillators, insulin pumps, and continuous glucose monitors.[2532]

In addition to MDRC, comments supporting this class were filed by Professor Matthew D. Green,[2533] Jay Freeman,[2534] Public Knowledge,[2535] Free Software Foundation

[2531] MDRC's proposed regulatory language reads as follows: "Computer programs, in the form of firmware or software, including the outputs generated by those programs, that are contained within or generated by medical devices and their corresponding monitoring systems, when such devices are designed for attachment to or implantation in patients, and where such circumvention is at the direction of a patient seeking access to information generated by his or her own device or at the direction of those conducting research into the safety, security, and effectiveness of such devices." MDRC Pet. at 1-2.

[2532] NPRM, 79 Fed. Reg. at 73,871.

[2533] Green Class 27 Supp.

("FSF"),[2536] New America's Open Technology Institute ("OTI"),[2537] Catherine Gellis and the Digital Age Defense project ("Gellis/Digital Age Defense"),[2538] and over 1600 individual commenters.[2539]

Based on the record as developed in the course of the proceeding, the Register concludes that Proposed Class 27 should be divided into Proposed Class 27A (Security and Safety Research) and Proposed Class 27B (Patient Data), so that the two distinct types of uses proponents seek to enable can be separately addressed. The discussion here will address only Proposed Class 27B, that is, circumvention to allow patient access to data generated by his or her own medical device and/or corresponding monitoring system.[2540] In addition, as discussed below, the record reveals that Proposed Class 27B does not actually focus on circumvention to access computer programs that are on medical devices or monitoring systems, but rather the data outputs generated by those programs. For this reason, the Office treats Proposed Class 27B as a proposal to circumvent access controls on protectable compilations of medical device data, which would fall into the more general class of literary works.[2541]

a. Background

At the outset, it is important to understand the devices, and the copyrighted works, that are encompassed by Class 27B. As noted above, the proposed exemption refers to "medical devices" and their "corresponding monitoring systems." MDRC explains that by "medical devices," it means, specifically, "devices that are physically implanted in whole or in part to the body and are used as part of the delivery of therapy and medical care to a patient," including pacemakers, ICDs, insulin pumps, and continuous glucose monitors.[2542] While in its petition MDRC also referred to "devices [that] are designed for

---

[2534] Freeman Class 27 Supp.

[2535] Public Knowledge Class 27 Supp.

[2536] FSF Class 27 Supp.

[2537] OTI Class 27 Reply.

[2538] Gellis/Digital Age Defense Class 27 Supp.

[2539] Digital Right to Repair Class 27 Supp. (1659 individuals); Gregory Borodiansky Class 27 Reply; Henry Feldman Class 27 Reply; Patrick Ferguson Class 27 Reply; Don Lowery Class 27 Reply; Bruce Schneier Class 27 Reply; Michael Weinberg Class 27 Reply.

[2540] Proposed Class 27A, which would permit research directed to security and software flaws in medical devices, is discussed with other analogous proposals elsewhere in the Recommendation.

[2541] *See* U.S. COPYRIGHT OFFICE, COMPENDIUM OF U.S. COPYRIGHT OFFICE PRACTICES § 503.1(BA) (3d ed. 2014) ("COMPENDIUM (THIRD)") (describing "compilations of information" as falling within the "literary work" category of authorship).

[2542] MDRC Supp. at 2. Pacemakers and ICDs are wholly implanted within the body, usually in the chest or the abdomen. *See Tests and Procedures: Pacemaker—Definition*, MAYO CLINIC, http://www.mayoclinic.org/tests-procedures/pacemaker/basics/definition/prc-20014279 (last visited Oct. 7, 2015); NAT'L HEART, LUNG, AND BLOOD INST., *What Is an Implantable Cardioverter Defibrillator?*, NAT'L INSTS. OF HEALTH, http://www.nhlbi.nih.gov/health/health-topics/topics/icd (last visited Oct. 7, 2015) ("NAT'L HEART, LUNG, AND BLOOD INST.") (cited in MDRC Supp. at App. C at ¶ 5 n.12). Insulin pumps, which consist of needles

attachment" as well as implantation in patients,[2543] MDRC's subsequent filings and the remainder of the record demonstrate that the proposed exemption is not intended to encompass attached devices that are neither wholly nor partially implanted, and MDRC specifically excludes "consumer health devices, such as digital pedometers and other devices that gather data and report their results directly to the patient."[2544] The term "[c]orresponding monitoring systems," in turn, refers specifically to devices such as handheld receivers or monitoring base stations, that wirelessly receive data from medical devices, and in some cases further relay that data to a centralized monitoring facility or to the physician.[2545] As used herein, then, the term "corresponding" or "personal" monitoring system refers to a portable or home device rather than a monitoring system that resides at a centralized facility or with a health care provider.[2546]

Proponents address continuous glucose monitors and ICDs as representative examples of the types of medical devices and monitoring systems that would be encompassed by the exemption. A continuous glucose monitor is an example of a "partially implanted" medical device. It tracks and reports a patient's glucose levels using a small, replaceable sensor that is inserted by the patient under the skin; the sensor is attached by wire to a transmitter that is outside the patient's body. The transmitter wirelessly relays glucose values on a periodic basis to a portable (handheld) "receiving computer" that displays certain information about a patient's glucose level.[2547] (In the case of a continuous glucose monitor, the sensor and transmitter together would constitute the "medical device," and the handheld receiving computer would be the "corresponding monitoring system," as those terms have been used in the proposed exemption.) The information displayed on the handheld receiving device, however, may not be comprehensive. Benjamin West, an independent researcher and member of MDRC, testified that his own continuous glucose monitor displays the current glucose

---

and tubing attached to the body that deliver insulin doses, and continuous glucose monitors, which consist of sensors placed under the skin, are only partially implanted, and can be described as temporary, as they often require replacement after a set period of days. *See* Jerome Radcliffe, *Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System*, BLACK HAT (2011), https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf ("Radcliffe") (cited in MDRC Supp. at 10 n.62); Tr. at 8:10-13 (May 29, 2015) (West, MDRC).

[2543] MDRC Pet. at 1.

[2544] MDRC Supp. at 2.

[2545] For background on monitoring systems, see *id*. at 5, 7-8, App. C; *see also* Tr. at 8:10-19 (May 29, 2015) (West, MDRC); Tr. at 53:11-13 (May 29, 2015) (Sellars, MDRC); Sherwin Siy, *Copyright Law and My Mother's Heart*, PUBLIC KNOWLEDGE (Jan. 20, 2015), https://www.publicknowledge.org/news-blog/blogs/copyright-law-and-my-mothers-heart ("*Copyright Law and My Mother's Heart*") (cited in MDRC Supp. at 11 n.68) (noting that data from a pacemaker and emergency defibrillator "are stored on the device itself," then "transferred to the base station, and then later transmitted to a monitoring company," which will notify the doctor of any pertinent information, or that alternatively data can be retrieved through direct interrogations by a doctor).

[2546] *See* Tr. at 48:02-09 (May 29, 2015) (Sellars, MDRC) (discussing monitoring devices not easily accessible by patients).

[2547] *Id.* at 8:10-19 (West, MDRC); *see also* Radcliffe (cited in MDRC Supp. at 10 n.62).

number and provides a general indication whether glucose levels have gone up or down since the last reading.[2548] He explained, however, that knowing the exact amount by which glucose levels had changed since the last reading is also significant.[2549]

ICDs, in turn, are small devices that are fully implanted in the chest or the abdomen that "regulate[] the beating of [the] heart and deliver[] shocks to treat life-threatening ventricular arrhythmias."[2550] ICD patient Hugo Campos explains that ICDs also monitor device battery life, the amount of time it takes to deliver a life-saving shock, a patient's heart rhythm and daily activity, and variations of chest impedances to see if there is a buildup of fluids in the chest, though such data is not immediately available to the patient.[2551] Instead, such patient data is recorded in the ICD, and can be reviewed by the patient only during periodic checkups with a doctor, who obtains the data either directly from the device using an "interrogation" tool largely available in hospitals or similar environments, or via a report that is generated by the device manufacturer or monitoring company, which receives the data through a monitoring system installed at the patient's home.[2552] As discussed below, proponents assert that immediate access to the data from an ICD can be valuable to a patient.

Proponents concede that, for purposes of accessing such patient data, they are not seeking to copy or modify firmware or software contained in their medical devices or corresponding monitoring systems[2553] and do not claim the need even to access such firmware or software.[2554] Instead, MDRC makes clear that it only seeks to access the "data outputs" that are generated by that firmware or software, and transmitted out of medical devices or monitoring systems, which it claims are capable of being intercepted but may be protected by TPMs.[2555] In other words, for purposes of Proposed Class 27B, MDRC is seeking to access data, not computer programs. Furthermore, MDRC appears

---

[2548] Tr. at 10:03-19 (May 29, 2015) (West, MDRC; Charlesworth, USCO).

[2549] *Id.* at 9:14-10:13 (West, MDRC; Charlesworth, USCO; Damle, USCO).

[2550] MDRC Supp. at App. C at ¶ 5; *see also* NAT'L HEART, LUNG, AND BLOOD INST. (cited in MDRC Supp. at App. C at ¶ 5 n.12).

[2551] Hugo Campos, *Hugo Campos Fights for the Right To Open His Heart's Data*, TED (Jan. 20, 2012), http://tedxtalks.ted.com/video/TEDxCambridge-Hugo-Campos-fight (cited in MDRC Pet. at 3 n.7); *see also* MDRC Supp. at App. C at ¶¶ 5-6.

[2552] MDRC Supp. at App. C at ¶¶ 1, 6; *see also Copyright Law and My Mother's Heart* (cited in MDRC Supp. at 11 n.68); Tr. at 48:02-09 (May 29, 2015) (Sellars, MDRC).

[2553] Tr. at 34:02-05 (May 29, 2015) (Sellars, MDRC) (stating that the "exemption here is seeking to access the . . . data outputs of the device, not to modify the software that is in the devices").

[2554] The Register notes that although the terms "firmware" and "software" are variously used throughout the Recommendation, both are "computer programs" within the meaning of the Copyright Act. *See* 17 U.S.C. § 101 (definition of "computer program").

[2555] MDRC Supp. at 4 (noting that the works in question for patient access to data are "the data outputs of these devices"); *see also* MDRC Reply at 4 ("Currently implanted or attached devices are only implicated by the proposed exemption in circumstances where patients seek to access their own data through the passive monitoring of data already being transmitted.").

to limit its request to circumvention of TPMs protecting wireless data outputs, explaining that the data would be accessed using "a form of radio transmission interception."[2556] Accordingly, although it appears that some personal monitoring systems referenced in MDRC's written comments transmit collected data to central locations via telephone lines,[2557] MDRC is seeking only to circumvent TPMs on wireless transmissions.

Proponents assert that an exemption is necessary because medical device manufacturers are increasingly applying TPMs to the data outputs of medical devices and monitoring systems.[2558] Even though some devices do not currently employ TPMs, proponents note that recent guidance issued by the Food and Drug Administration ("FDA") recommends that manufacturers impose TPMs to protect device security and patient privacy, such as by limiting access to data through passwords, code authentication, and encryption of wireless communications.[2559] Proponents assert that those recommendations are likely to be adopted by the medical device industry and lead to an increase in the application of TPMs; they explain that "[g]uidance documents like these, while not legally binding, are the usual means by which the FDA indicates its

[2556] MDRC Supp. at 10; *see also* MDRC Reply at 4 & n.15 (explaining that the exemption would be limited to "passive monitoring of data already being transmitted" through "a form of radio transmission interception"). At the public hearing, a representative from MDRC made a passing reference to the use of "hardware or software USB sniffers" to access data held on the handheld receiving computer of a continuous glucose monitor. *See* Tr. at 8:22-9:04 (May 29, 2015) (West, MDRC) ("[W]e used a combination of hardware and software USB sniffers to create a transcript of the interactions that the vendor typically has with these devices."); *see also* MDRC Supp. at App. F at ¶ 2 (referencing investigation of "USB . . . protocols" without elaboration). The Register understands the USB standard to be a protocol for communication over physical cables. MDRC's written submissions, however, are clearly limited to "passive monitoring of data already being transmitted," MDRC Reply at 4, and do not indicate any desire to circumvent access controls on wired communications for that purpose.

[2557] *See* MDRC Supp. at App. C at ¶ 6; *How the CareLink Network Works*, MEDTRONIC, (Mar. 26, 2014), http://www.medtronic.com/patients/sudden-cardiac-arrest/living-with/carelink/how-it-works/index.htm (cited in MDRC Supp. at App. C at ¶ 6 n.15); *see also* Daniel Halperin et al., *Security and Privacy for Implantable Medical Devices*, 7 IEEE: PERVASIVE COMPUTING 30, 32-33 & fig. A (2008) ("Halperin et al.") (cited in MDRC Supp. at 2 n.4) (explaining that "major pacemaker and ICD manufacturers now produce at-home monitors that wirelessly collect data from implanted devices and relay it to a central repository over a dialup connection," which is depicted as a telephone or internet protocol network).

[2558] MDRC Supp. at 3; *see also* Public Knowledge Class 27 Supp. at 1; Tr. at 60:08-12 (May 29, 2015) (West, MDRC); Tr. at 17:01-08 (May 29, 2015) (Sellars, MDRC) (noting that "on many devices that are on the market today and on more that are coming out in the near future, even accessing the data itself would mean circumventing a technological protection measure").

[2559] MDRC Supp. at 7, 9 (citing FDA, CONTENT OF PREMARKET SUBMISSION FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 4 (Oct. 2, 2014), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulation andGuidance/GuidanceDocuments/UCM356190.pdf and FDA, RADIO FREQUENCY WIRELESS TECHNOLOGY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 10-11 (Aug. 14, 2013), *available at* http://www.fda.gov/downloads/MedicalDevices/Device RegulationandGuidance/GuidanceDocuments/ucm077272.pdf).

preferences when examining devices, and entities regulated by the FDA routinely treat these guidelines as rules in order to assure expediency in FDA approvals."[2560]

Proponents point to a few types of TPMs that restrict access to the wireless data outputs of medical devices and monitoring systems, including encryption systems that require a private decryption key and proprietary readers that are necessary in order to access device information.[2561] MDRC explains that, once the radio transmissions from the device are intercepted, "reverse engineering techniques" can be employed to decode device outputs communicated along radio frequencies transmitted by medical devices.[2562]

One threshold question raised by the Office in the NPRM is whether the data outputs of medical devices and corresponding monitoring systems constitute copyright-protected material.[2563] MDRC observes that "based on current caselaw, it is likely that many of the outputs in question here are not protectable," and that the prohibition on circumvention in section 1201 would thus not apply to efforts to circumvent TPMs on that data.[2564] MDRC elaborates that "[i]n most cases the data consists principally of the readouts of sensors gathering information on the physical characteristics of the patient and records of device activity, including the patient's name, the treating physician's name, information about the date of installation, and other facts that may be relevant to the patient's care."[2565] MDRC acknowledges that such data "reveals nothing more than a fact of nature, which, like an idea, is not protectable unless embodied in an original expression."[2566] MDRC also notes that a comprehensive readout of data collected by the medical device would show "no selection of information, a requirement for protection of a compilation of data."[2567] Furthermore, MDRC states that the transmission of data "may not be sufficiently 'fixed' to be a protectable work if they are not being saved simultaneously with their transmission."[2568]

But while this may be the most typical scenario, MDRC expresses concern that some data outputs "may have the necessary original selection and arrangement to be protectable expressions, [even if] the protection is quite thin."[2569] For example, MDRC

[2560] *Id.* at 9.

[2561] *See, e.g.*, *id.* at 7-9; Public Knowledge Class 27 Supp. at 1.

[2562] MDRC Supp. at 10.

[2563] NPRM, 79 Fed. Reg. at 73,871 (asking commenters to address "[w]hether the outputs generated by the medical device programs constitute copyright-protected materials").

[2564] MDRC Supp. at 4.

[2565] *Id.* at 5.

[2566] *Id.*

[2567] *Id.*

[2568] *Id.*

[2569] *Id.* at 4-5 (citing *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 358 (1991) and *CCC Info. Sys., Inc. v. Maclean Hunter Market Reports, Inc.*, 44 F.3d 61, 67 (2d Cir. 1994) for the proposition that a selection and arrangement of data may be protected by copyright).

asserts that data outputs on devices can be transmitted as batch reports "from the device either on a set schedule or when prompted by a wired or wireless connection to [a] device reader."[2570] It also suggests that "a collection of data sent as a batch report could be protectable, if it can be shown that it was assembled with a degree of originality in the selection and arrangement of the information."[2571] MDRC further asserts that "it is often not possible for a researcher to know whether a dispatch report contains protectable expression or not until after the researcher circumvents any TPM over that data," which is likely to hold true for patients circumventing their devices as well.[2572] Consequently, MDRC notes that accessing such protectable data outputs "may raise anticircumvention issues,"[2573] and urges the Register to recommend an exemption to cover situations where the data output is copyrightable as a compilation. In this regard, the Register observes that none of the opponents dispute that some data outputs, such as in the form of batch reports, might be copyrightable, and that one opponent, Advanced Medical Technology Association ("AdvaMed"), expressly claims that "the structure, format, and arrangement of the output data" could be protectable.[2574]

b. Asserted Noninfringing Uses

Proponents assert that, to the extent data outputs are protectable under copyright, patient access to that data constitutes a fair use. Under the first factor, the purpose and character of the use, MDRC argues that making copies of lawfully acquired material "underlying unprotectable data" is often considered fair.[2575] Proponents further assert that giving a patient access to the data outputs from his or her own device should be favored because it allows the patient to evaluate whether the device is working.[2576] Though not in the context of addressing fair use, MDRC observes that patients can use the data to "determine whether a medical emergency is occurring."[2577] By way of illustration, MDRC provided the statement of a patient with an ICD who explained that immediate access to the data being output from his device could help him instantly detect

[2570] *Id.* at 5; *see also* Halperin et al. at 30, 33 & fig. B (cited in MDRC Supp. at 2 n.4); Tr. at 18:16-25 (May 29, 2015) (Sellars, MDRC) ("I would also note in some devices, the data is not streamed in real time, it's dispatched, and when there is a dispatch of data, there is often a greater affordance for an arrangement or selection of particular information. Also, sometimes this data will include metadata about the patient, including who their primary care physician is, who they are, their date of birth, and other information that might be relevant to their care.").

[2571] MDRC Supp. at 6 & n.37.

[2572] *Id.* at 6-7.

[2573] *Id.* at 5.

[2574] AdvaMed Class 27 Opp'n at 5 (citing *Eng'g Dynamics, Inc. v. Structural Software, Inc.*, 26 F.3d 1335, 1345 (5th Cir. 1994) and *Positive Software Solutions, Inc. v. New Century Mortgage Corp.*, 259 F. Supp. 2d 531, 535 (N.D. Tex. 2003)).

[2575] MDRC Supp. at 13 & nn.87-88 (citing *Assessment Techs. of Wisconsin, LLC v. WIREdata, Inc.*, 350 F.3d 640, 645 (7th Cir. 2003)).

[2576] *See, e.g.*, Public Knowledge Class 27 Supp. at 2.

[2577] MDRC Supp. at 3.

problems, for example, "an automatic switch in pacing mode" that "may indicate the onset of atrial fibrillation, a common arrhythmia that increases a person's risk of having an ischemic stroke," or "a sudden change in lead impedance" that might "indicate a serious device malfunction that can lead to inappropriate shocks to the heart."[2578] Public Knowledge urges that "the purpose[] of improving the health and well-being of individual circumventing patients" should weigh in favor of fair use.[2579]

Proponents assert that the second fair use factor similarly weighs in favor of a finding of fair use, because even where data outputs are selected and organized in a manner that renders them protectable, the copyright protection is "thin."[2580] Public Knowledge further notes that the data outputs "are functional in nature, containing arguable amounts of creative expression mixed with unprotectable facts and functional elements."[2581]

With respect to the third fair use factor, proponents acknowledge that in some cases they might be accessing an entire work.[2582] Public Knowledge nonetheless asserts that any use of copyrightable expression would fall under fair use because even "using the totality of a work is never a bar to a finding of fair use."[2583] Additionally, Public Knowledge contends that proponents would not be copying and using the data structures in and of themselves, but instead would be using "the output data to convey the raw information contained within any data structures."[2584] MDRC further argues that "to the extent one must make a copy to reveal the underlying [uncopyrightable] data, courts give that incidental copying latitude."[2585]

Proponents assert that the fourth factor also weighs in favor of fair use, because use of the data does not supplant market demand for, or harm the value of, the data outputs, or the software or devices that generate those outputs.[2586] MDRC argues that any copies made to access underlying unprotectable data neither supplant patient need for the medical devices themselves, nor the "need for the reports that medical device companies may generate with the same underlying data, which are combined with other

---

[2578] *Id.* at App. C at ¶ 8.

[2579] Public Knowledge Class 27 Reply at 3; *see also* Public Knowledge Class 27 Supp. at 2 ("[P]ursuing the safety, security, or effectiveness of [a] device . . . should categorically also be considered fair, based upon the literal lifesaving purpose of the use.").

[2580] MDRC Supp. at 4-5.

[2581] Public Knowledge Class 27 Reply at 3.

[2582] *See id.*; MDRC Reply at 21-22.

[2583] Public Knowledge Class 27 Reply at 3 (citing *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 586-87 (1994) and *Perfect 10, Inc. v. Amazon, Inc.*, 508 F.3d 1146, 1167-68 (9th Cir. 2007)).

[2584] *Id.* at 4.

[2585] MDRC Supp. at 15 (citing *WIREdata*, 350 F.3d at 644-45 and *Golan v. Holder*, 132 S. Ct. 873, 890 (2012)).

[2586] *See id.* at 23; MDRC Reply at 5; Public Knowledge Class 27 Reply at 3.

information and presented in tandem with a consultation from a physician."[2587] Public Knowledge also argues that proponents' desired uses would not supplant the market for or diminish the value of medical device software because patients will have already purchased the software by buying the device.[2588] Public Knowledge also questions whether there is a market at all for "the software itself, as opposed to the devices that contain it."[2589] Proponents did not separately address potential effects on the market for corresponding monitoring systems or software on those systems. But they generally treated monitoring systems as necessary incidents to the medical devices themselves, suggesting the view that the market for medical devices and that of corresponding monitoring systems are essentially the same.

Finally, MDRC observes that "[c]ourts are empowered to consider other factors in a fair use determination," and urges that "in the particular case of accessing one's own data from a medical device, it's entirely possible that a court would take into account the highly personal and potentially life-saving nature of the information in question."[2590]

c. Asserted Adverse Effects

Proponents argue that the prohibition on circumvention adversely affects their desired uses because, absent an exemption to cover potentially protected data outputs, they would have only limited access to their personal medical data. For example, in the case of ICDs, proponents note that important medical data is only accessible at periodic checkups with a doctor, as explained above. This is often inadequate since patients may receive pertinent information months after their "devices . . . detect time-sensitive anomalies that patients may not feel, including changes in heart rhythm or blood flow."[2591] In addition, not only do patients have to schedule a consultation with their doctors, but the reports created by device manufacturers or monitoring companies are sometimes only shared with the patient "for a fee."[2592]

[2587] MDRC Supp. at 14 (asserting that the "uses of data advocated here instead concern time-sensitive access for safety and security reasons, including detecting anomalies and emergencies, or sharing time sensitive medical information with family members as part of their care"); *see also* MDRC Reply at 5 ("[T]he types of uses considered in this exemption would never supplant the need for the original device in any conceivable use case. No cardiac patient would look at a device's source code in lieu of getting a pacemaker; no patient with diabetes would look at the data readout from an insulin pump instead of getting one."); Tr. at 27:02-11 (May 29, 2015) (Sellars, MDRC).

[2588] Public Knowledge Class 27 Reply at 3.

[2589] *Id.*

[2590] MDRC Supp. at 14-15.

[2591] MDRC Reply at 9-10; *see also* Public Knowledge Class 27 Reply at 6 (contending that accessing data through doctors or other medical professionals is not a viable alternative to accessing it directly from the device because such devices have "vital information whose relevance and importance—such as blood sugar levels or heart rhythms—are often immediate").

[2592] MDRC Supp. at App. C at ¶ 6.

Proponents also contend that, if patients are able more easily to access their own medical data, such access will improve patient care by allowing patients to immediately detect major health risks,[2593] thus facilitating highly personalized treatment,[2594] giving patients better ability to oversee their own health,[2595] and providing both patients and their doctors with more timely information on physiological events occurring within the body.[2596] For instance, Campos, the ICD patient mentioned above, explained that "manually logging symptomatic cardiac episodes led me to identify the consumption of Scotch whisky as a trigger for atrial arrhythmias, and of caffeine as seemingly not harmful," but that he could track his health at a more granular level if the data generated by the ICD were more readily available to him for analysis.[2597] West, the patient with the continuous glucose monitor, explained that while his handheld receiving computer indicates his current glucose level and whether that level is higher or lower than the last glucose reading, knowing as well the exact level of change from the prior reading is a "very important cue" in helping him manage his disease.[2598]

d. Argument Under Statutory Factors

Proponents argue that the statutory factors set forth in section 1201(a)(1) support granting this exemption as well. Regarding the first factor, the availability for use of copyrighted works, MDRC notes that the use of works for medical treatment "does not depend on the presence or absence of TPMs" because it is undertaken by the patient out of necessity.[2599] MDRC thus maintains that the availability of either the data outputs or the software running a medical device would not be affected by an exemption because "the device and copyrighted work are inseparable."[2600]

For the second factor, MDRC argues that availability for use for nonprofit, archival, preservation and educational purposes is negatively impacted by the prohibition on circumvention because "there are no alternatives [to circumvention] for time-sensitive

---

[2593] *See, e.g.*, *id.* at 3, 19; Public Knowledge Class 27 Supp. at 7 (contending that the "inability of patients . . . to access networked medical devices creates clear and present harms for them," as even instances where such harms begin as "mere inconvenience[s]" can "over the duration of a course of treatment, escalate into a grave barrier"); MDRC Reply at 9.

[2594] *See, e.g.*, MDRC Reply at 7; *see also* Tr. at 56:03-12 (May 29, 2015) (Sellars, MDRC).

[2595] *See, e.g.*, MDRC Reply at 10 (stating that patients' access to data on the amount of insulin being released from insulin pump can give patients better ability to care for themselves); Freeman Class 27 Supp. at 1; *see also* Tr. at 11:12-12:11 (May 29, 2015) (West, MDRC).

[2596] *See, e.g.*, MDRC Supp. at 19 ("At the individual level, physiological events that could be critical to a patient's well-being may be missed if the device detects the event but does not inform the patient."); Freeman Class 27 Supp. at 1; MDRC Reply at 10-11; *see also* Tr. at 14:13-15:18 (May 29, 2015) (West, MDRC).

[2597] MDRC Supp. at App. C at ¶ 9.

[2598] Tr. at 9:11-19, 10:03-13 (May 29, 2015) (West, MDRC).

[2599] MDRC Supp. at 23 ("[I]f a person needs an insulin pump, they get an insulin pump.").

[2600] *Id.*

access to a patient's data for purposes of detecting device flaws or life-threatening events."[2601] It further notes the existence of programs and websites that allow patients to share their data to better understand and study the data as well as their own health.[2602] With respect to the third factor, MDRC asserts that medical device users having greater access to their medical data will enable them, as well as others through the sharing of the data, to engage in more research, reporting, and commentary about health issues.[2603]

As for the fourth factor, MDRC contends that "showing ways that patients can leverage the data gathered on these devices to prevent adverse incidents and improve their health" will increase market demand for medical devices (and the software contained therein).[2604] Public Knowledge also notes, in the context of its fair use argument, that circumvention for purposes of access to device software that has already been paid for would not substitute for the market for or negatively affect the value of that software.[2605]

With respect to other factors that may be considered by the Librarian, proponents respond to opponents' concerns, discussed below, that an exemption could have potential impacts on health, safety, and security by noting that other laws, such as the Computer Fraud and Abuse Act ("CFAA"), which prohibits unauthorized access of certain protected computer systems,[2606] and the Health Insurance Portability and Accountability Act ("HIPAA"), which protects private health information from unauthorized disclosure,[2607] might prevent any unwanted or malicious actions.[2608] At the same time, proponents point out that HIPAA does not preclude patients from accessing their own medical data or choosing to share it with third parties.[2609] Proponents further contend that "the Librarian and the Office are ill equipped to make determinations about privacy and patient safety," and that FDA is the correct administrative body to regulate in these areas.[2610] Proponents thus urge the Librarian and the Office to "remove the potential impediments of Section

[2601] *Id.* at 24.

[2602] MDRC Reply at 12.

[2603] *See* MDRC Supp. at 24, App. C; *see also* MDRC Reply at 12 (noting that one patient who was able to access his own medical data has made it "publicly available so others may use it to conduct further research").

[2604] MDRC Supp. at 25.

[2605] Public Knowledge Class 27 Reply at 3.

[2606] 18 U.S.C. § 1030.

[2607] 42 U.S.C. § 1320d-6.

[2608] *See* Tr. at 43:20-44:02 (May 29, 2015) (Sellars, MDRC) (asserting that "other laws could fill in the gap for bad actors"); *see also* Public Knowledge Class 27 Post-Hearing Resp. at 3-4.

[2609] *See* Public Knowledge Class 27 Reply at 9 (contending that "[n]either HIPAA, nor any other privacy statute, prevents patients from disclosing their own records to third parties directly" or authorizing third parties to make use of such information); *see also* MDRC Post-Hearing Resp. at 4-5 (asserting, for example, that the proposed exemption is not in conflict with the CFAA since the exemption "requires consent from a patient if the device is used in that patient's care").

[2610] Public Knowledge Class 27 Reply at 9; MDRC Reply at 18-20.

1201" by granting an exemption so that the appropriate agency can more practically decide these issues.[2611] Public Knowledge also argues that concerns expressed by opponents about the exposure of trade secrets are irrelevant to copyright interests and are "no part of the statutory factors for determining an exemption."[2612]

As is also discussed below, opponents raise issues regarding the impact of the exemption on the battery life and performance of implanted devices due to more frequent queries for data readouts. MDRC explains that it "is not asking for continuous interrogation of devices," but instead only "to be able to intercept and read" the data already periodically dispatched by the devices.[2613] Public Knowledge suggests, however, that the exemption should also permit more active access through on-demand querying of the device, claiming that there is likely to be "minimal effect" from such activity and that any remaining concerns can easily be remedied by merely changing the device's battery.[2614] But Public Knowledge does not provide any specific evidence on the parameters of, or the need for, such increased access, or the feasibility of battery replacement.[2615]

Finally, proponents suggest that the prohibition on circumvention is interfering with patients' rights to and ownership of their medical data by isolating them from their own data and preventing them from using it to learn more about their health.[2616]

2. Opposition

The Office received comments in opposition to the proposed exemption from AdvaMed, Intellectual Property Owners Association ("IPO"), LifeScience Alley, and National Association of Manufacturers ("NAM").[2617]

a. Asserted Noninfringing Uses

Citing *Engineering Dynamics, Inc. v. Structural Software, Inc.*, which held that user input and output formats for a computer system are copyrightable,[2618] and *Positive Software Solutions, Inc. v. New Century Mortgage Corp.*, which held the same for data

[2611] Public Knowledge Class 27 Reply at 9; *see also* MDRC Reply at 18 (asserting that in a case where the authority of FDA and the Office overlap, "the most effective response is for each agency to regulate according to its expertise, and avoid duplicative efforts").

[2612] Public Knowledge Class 27 Reply at 10.

[2613] MDRC Reply at 11; *see also* Public Knowledge Class 27 Reply at 8 (noting that "[a]ccessing data already being transmitted by the device on its own schedule will have no effect upon its ordinary operation").

[2614] Public Knowledge Class 27 Reply at 8; *see also* Tr. at 47:13-19 (May 29, 2015) (Sellars, MDRC).

[2615] *Id.*

[2616] MDRC Supp. at 3; MDRC Reply at 8-12; Public Knowledge Class 27 Reply at 6.

[2617] AdvaMed Class 27 Opp'n; IPO Class 27 Opp'n; LifeScience Alley Class 27 Opp'n; NAM Opp'n.

[2618] 26 F.3d at 1345 (addressing user input and output formats).

structures in a database,[2619] AdvaMed asserts that "copyright protection in device outputs may extend to, for example, the structure, format, and arrangement of the output data."[2620] But AdvaMed does not elaborate on these precedents or provide any examples of output data that it claims are copyrightable.

Even assuming that some outputs may be copyrightable, opponents present little argument to counter proponents' assertion that patient access to such medical data transmitted from a device or its corresponding monitoring system would constitute a noninfringing fair use of such works. AdvaMed makes the bare assertion that "[t]he analysis of any use of the copyrighted works arguably points against the proposed uses falling under the fair use exception;"[2621] it does not explain this point or conduct a factor-by-factor analysis of fair use for the proposed activity of patient access.

b. Asserted Adverse Effects

Opponents concede that "patients have the inherent right to access their own medical data,"[2622] but contend that alternatives to unauthorized circumvention exist such that proponents suffer no adverse impact resulting from the prohibition.[2623] Specifically, proponents assert that "[s]uch data access rights can be exercised (and already are provided) through health care providers having the appropriate tools and training to collect and protect patient data without compromising the safety and longevity of [the patient's] device."[2624] NAM further asserts that "[p]roponents have offered no evidence that patients are unable to obtain their data from qualified medical professionals when requested."[2625] Accordingly, NAM posits that the inability of patients to directly access their data through circumvention "is not the type of 'distinct, verifiable, and measurable' adverse impact that warrants an exemption to the prohibition."[2626]

c. Argument Under Statutory Factors

Regarding the first statutory factor, concerning the availability of copyrighted works, opponents assert that the prohibition on circumvention is not harming the ability for patients to access their personal medical data because "[c]urrently the patient has access to their data through their physician."[2627] Opponents present no argument with

[2619] 259 F. Supp. 2d at 535 (addressing Structured Query Language data structures).

[2620] AdvaMed Class 27 Opp'n at 5.

[2621] *Id.*

[2622] *Id.* at 2.

[2623] *See, e.g.*, NAM Opp'n at 5-6; IPO Class 27 Opp'n at 2; LifeScience Alley Class 27 Opp'n at 4, 6; AdvaMed Class 27 Opp'n at 2.

[2624] AdvaMed Class 27 Opp'n at 2; *see also* LifeScience Alley Class 27 Opp'n at 4.

[2625] NAM Opp'n at 5.

[2626] *Id.* at 6.

[2627] LifeScience Alley Class 27 Opp'n at 6; *see also* IPO Class 27 Opp'n at 2; AdvaMed Class 27 Opp'n at 2; NAM Opp'n at 5-6.

respect to the second and third factors. As for the fourth factor, which considers market impact, AdvaMed suggests that the proposed exemption will devalue medical devices, and impliedly the software and data outputs generated by such devices, by causing the public to believe that devices can be accessed or controlled by unauthorized parties and, as a result, are insecure or unsafe.[2628] However, like proponents, opponents do not separately address how an exemption would affect the market for or value of any corresponding monitoring systems or data outputs.

Opponents place much weight on the fifth statutory factor, allowing the Register and Librarian to consider such other factors as may be appropriate. Opponents contend that allowing users to circumvent medical device access controls—to the extent they exist now and as they become more prevalent in the future—will be at best unsafe and even potentially life-threatening. As a threshold matter, opponents maintain that the proposed exemption is overly broad in that it could include many different types of devices, making it "difficult to appraise the full scope or risks likely to be created."[2629] But more generally, both here and in relation to the issue of security research addressed in Class 27A, opponents take the position that circumvention should not be allowed for any medical device that currently is or in the future will be used in patient care, including implanted devices. Opponents contend that tampering and unauthorized circumvention could result in malfunction, corruption of data, degradation, or damage, and thus present "an unnecessarily high risk to patient safety."[2630] Notably, this line of argument seems to assume that circumvention of the computer software on the devices themselves would be necessary. As explained above, however, and as clarified during the proceeding, it appears that the circumvention actually sought by proponents would permit access only to data outputs from devices or monitoring systems, rather than the devices or systems themselves.

Opponents further contend that requesting data from devices at an abnormally high rate could result in serious injury or death, as telemetry sessions conducted when devices are "in a communication mode" drastically reduces their overall battery life and could cause them to stop performing critical functions prematurely.[2631] Thus, in AdvaMed's view, "[i]f the Copyright Office were to advance an exemption permitting unauthorized circumvention activity for a patient to study his or her own device, it should be limited to the passive monitoring of radio transmissions that are produced by the device in its unaltered operating form."[2632] In addition, LifeScience Alley argues that allowing medical device users to have greater access to their medical data "will directly

[2628] AdvaMed Class 27 Opp'n at 7.

[2629] *Id.* at 4; *see also* IPO Class 27 Opp'n at 2; NAM Opp'n at 2.

[2630] AdvaMed Class 27 Opp'n at 4; *see also* LifeScience Alley Class 27 Opp'n at 4 (noting that "[a]ny compromise of the proper operation of the software on a medical device could easily lead to patient death"); NAM Opp'n at 7.

[2631] *See, e.g.*, AdvaMed Class 27 Opp'n at 2; LifeScience Alley Class 27 Opp'n at 4; NAM Opp'n at 7.

[2632] AdvaMed Class 27 Opp'n at 3.

interfere with the doctor-patient relationship – in effect inducing patients to make decisions without the support of their doctor."[2633]

Opponents further assert that allowing circumvention could compromise personally identifiable or protected health information of both the patient who owns the device as well as other patients. Opponents suggest, without much elaboration, that granting this exemption could allow a malicious actor to access patient data by remotely connecting to a device, a device's corresponding monitoring system, or any associated networked system, all without permission from the patient or the device manufacturer.[2634] Opponents also maintain that unauthorized circumvention for the purpose of obtaining personal medical data could violate HIPAA by compromising patient privacy or contravene laws governing unauthorized access to computer systems.[2635] AdvaMed additionally argues that an exemption could potentially "provide wrongdoers with knowledge of how to manipulate and interface with the devices," thus enabling malicious hacking activities that could harm patients.[2636] And opponents contend that allowing circumvention "poses trade secret concerns" because it could allow access to device firmware and outputs without having to request authorization from, or enter into a contractual relationship with, the device manufacturer.[2637]

Finally, opponents urge the Office to "confer with the FDA and defer to its view in this matter, as FDA is the federal agency charged with assuring the safety, efficacy, and security of medical devices."[2638]

3. Discussion

The Register finds that proponents have made a sufficient showing that medical device manufacturers are using TPMs to control access to the data outputs transmitted by such devices and related systems.[2639] The Register also concludes that the record demonstrates that the use of TPMs will likely increase in the next three years, particularly in light of the new guidance issued by FDA.[2640]

The Register further agrees with proponents that, to be protected by copyright, the data output generated by a patient's medical device must reflect a "collection and

---

[2633] LifeScience Alley Class 27 Opp'n at 6.

[2634] *See, e.g.*, AdvaMed Class 27 Opp'n at 2, 4-5; IPO Class 27 Opp'n at 3; LifeScience Alley Class 27 Opp'n at 4, 6.

[2635] AdvaMed Class 27 Opp'n at 4, 7; IPO Class 27 Opp'n at 3.

[2636] AdvaMed Class 27 Opp'n at 7.

[2637] *Id.*; *see also* LifeScience Alley Class 27 Opp'n at 5.

[2638] AdvaMed Class 27 Opp'n at 7; *see also* NAM Opp'n at 2; IPO Class 27 Opp'n at 2-3; LifeScience Alley Class 27 at 2.

[2639] *See* MDRC Supp. at 3, 7-9; *see also* Public Knowledge Class 27 Supp. at 1.

[2640] *See* MDRC Supp. at 7, 9; Tr. at 17:01-08 (May 29, 2015) (Sellars, MDRC); Tr. at 60:08-12 (May 29, 2015) (West, MDRC).

assembling of . . . data that are selected, coordinated or arranged in a way that the resulting work as a whole constitutes an original work of authorship."[2641] Although the record is not as specific as it could be concerning the precise nature of data outputs generated by various medical devices, it seems safe to assume that in many cases, these outputs would simply reflect an unoriginal stream of data consisting of facts about the patient's physiological condition.[2642] If that were always the case, there would be no need for an exemption under section 1201(a)(1), because the outputs would not be protected under title 17.[2643]

But the record also indicates that some data outputs produced by medical devices—for example, batch-type reports—might qualify for protection as literary works if they reflect a sufficiently original selection and presentation of data.[2644] And

---

[2641] 17 U.S.C. § 101 (definition of "compilation"); s*ee also Feist*, 499 U.S. at 348 (asserting that factual compilations can be copyrightable where "even a directory that contains absolutely no protectable written expression, only facts, meets the constitutional minimum for copyright protection if it features an original selection or arrangement"); *CCC v. Maclean*, 44 F.3d at 65-66; COMPENDIUM (THIRD) §§ 312.2, 508.1.

[2642] *See, e.g.*, *Feist*, 499 U.S. at 363 (finding that listing telephone subscribers in alphabetical order was not original or creative in the coordination and arrangement of these facts since doing so is "an age-old practice, firmly rooted in tradition and so commonplace that it has come to be expected as a matter of course"); *Matthew Bender & Co., Inc. v. West Pub. Co.*, 158 F.3d 674, 682, 688-89 (2d Cir. 1998) (determining that a compilation of data is not copyrightable where the selection is dictated by industry conventions or other external factors or where "the author made obvious, garden-variety, or routine selections"); *BanxCorp. v. Costco Wholesale Corp.*, 978 F. Supp. 2d 280, 301, 307 (S.D.N.Y. 2013) (finding that data constitute unprotectable facts if they "purport[] to represent actual objective prices of actual things in the world" or discover merely "an 'empirical reality'").

[2643] *See* 17 U.S.C. § 1201(a)(1)(A) (providing that "[n]o person shall circumvent a technological measure that effectively controls access *to a work protected under this title*" (emphasis added)); *see also* 2012 Recommendation at 14-15 (concluding that an exemption for access to public domain literary works was unnecessary).

[2644] *See* COMPENDIUM (THIRD) § 508.1 (noting that a compilation "'results from a process of selecting, bringing together, organizing, and arranging previously existing material of all kinds, regardless of whether the individual items in the material have been or ever could have been subject to copyright'" (quoting H.R. REP. NO. 94-1476, at 57 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5670)); *see also CCC v. Maclean*, 44 F.3d at 67-68 (finding that the selection and arrangement of data in a database of used vehicle prices were sufficiently original because of plaintiff's presentation of independent predicted valuations for regions and the selection and presentation of optional features); *Mason v. Montgomery Data, Inc.*, 967 F.2d 135, 141-42 (5th Cir. 1992) (finding plaintiff's maps to be original and copyrightable because plaintiff independently selected which information from conflicting sources to include on his maps); *Key Publ'ns, Inc. v. Chinatown Today Publ'g Enters., Inc.*, 945 F.2d 509, 513-14 (2d Cir. 1991) (finding a directory of New York businesses to be sufficiently original because the plaintiff had exercised "judgment in choosing which facts from a given body of data to include," such as excluding businesses that the plaintiff thought would not remain open for long and creatively arranging the businesses in categories); *Kregos v. Associated Press*, 937 F.2d 700, 704-05 (2d Cir. 1991) (reversing a summary judgment dismissal of a copyright claim in a baseball pitching form, holding that the form had sufficient creativity in the selection of nine specific pitching statistics out of many to display, particularly in comparison to other pitching forms that only used at most three pitching statistics); 2000 Final Rule, 65 Fed. Reg. at 64,566 (noting that databases "that contain a significant amount of uncopyrightable material . . . , may nonetheless be covered by copyright by virtue of the selection, coordination and arrangement of the materials").

proponents confirm that certain types of devices and systems do in fact dispatch data in batches rather than in real time.[2645] Given the fact that opponents themselves argue that such outputs may be subject to copyright,[2646] the Register credits proponents' assertions that some outputs may be protectable.[2647]

Accordingly, the Register finds that proponents have adequately demonstrated that patients' access to their own medical data as embodied in protectable data compilations generated by implanted medical devices and corresponding home monitoring systems is likely to be hindered by TPMs that control access to that data. As explained below, they have also established that the activities proponents seek to carry out are likely to constitute noninfringing fair uses. As also discussed below, on the whole—though with important qualifications—the statutory factors set forth in section 1201(a)(1) tend to favor proponents.

a. Noninfringing Uses

The Register concludes that the overall record generally supports proponents' claim that accessing personal medical data is likely to be noninfringing as a fair use under section 107. Additionally, the Register notes that opponents did not make any meaningful attempt to rebut proponents' fair use claims.

Regarding the first fair use factor, the record establishes that the purpose and character of the proposed use favor a finding of fair use. The record reflects that proponents' desired uses will be personal and noncommercial since the proposed exemption seeks to allow patients to access potentially life-saving data for their own use, rather than for any monetary gain.[2648] In addition, allowing patients to access this data is likely to foster patients' research into their own conditions, as with the example provided by Campos, who discovered that consuming certain foods was associated with adverse health effects.[2649] Patients' ability to access their own data may also foster more general

[2645] *See* MDRC Supp. at 5, 6 & n.37; Halperin et al. at 30, 33 & fig. B (cited in MDRC Supp. at 2 n.4) (example of batch report transmitted by medical devices and home monitoring system); Tr. at 18:16-25 (May 29, 2015) (Sellars, MDRC).

[2646] *See* AdvaMed Class 27 Opp'n at 5 (citing *Eng'g Dynamics v. Structural Software*, 26 F.3d at 1345 and *Positive Software Solutions*, 259 F. Supp. 2d at 535).

[2647] *See Feist*, 499 U.S. at 348 (holding that factual compilations may be copyrightable where the "choices as to selection and arrangement, so long as they are made independently by the compiler and entail a minimal degree of creativity, are sufficiently original that Congress may protect such compilations through the copyright laws").

[2648] *See Harper & Row Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 562 (1985) (holding that "[t]he crux of the profit/nonprofit distinction is not whether the sole motive of the use is monetary gain but whether the user stands to profit from exploitation of the copyrighted material without paying the customary price").

[2649] MDRC Supp. at App. C at ¶ 9.

scholarship or research into specific medical conditions and technologies to the extent patients wish to share that data with others.[2650]

Furthermore, as Public Knowledge notes, even if the data is output in a manner that reflects some creative selection or arrangement, it seems that the patient would not be copying the outputs because of the value of that selection or arrangement *per se*, but simply to gain access to "the raw information contained *within* any data structures."[2651] In other words, the purpose of the use is to obtain access to the underlying and uncopyrightable factual information contained within the data output to allow additional use and analysis. That logic is supported to some extent by the Seventh Circuit's decision in *Assessment Technologies of Wisconsin, LLC v. WIREdata, Inc.*, cited by MDRC.[2652] In *WIREdata*, the defendant wanted to extract unprotectable data about properties that plaintiff had compiled into a database, and provide it to real estate brokers.[2653] In ruling for the defendant, the court stressed that "the only purpose of the copying would be to extract noncopyrighted material."[2654] Similarly, here, to the extent that access to noncopyrightable patient data requires copying of a protected compilation of such data, the Register does not find this to override the highly personal, noncommercial and research-oriented nature of the uses at issue.[2655] Moreover, to the extent the data is being reinterpreted and/or recompiled to allow more insights into a patient's health status, the use may well be a transformative one.[2656]

The second factor, the nature of the works, weighs in favor of fair use. As noted above, even if data outputs are copyrightable, they are nonetheless highly factual in nature; any copyright protection extends only to the selection and arrangement of the data and not to the data itself, which is the focus of the use.

[2650] *See* 17 U.S.C. § 107; MDRC Reply at 12.

[2651] Public Knowledge Class 27 Reply at 4 (emphasis added); *see also* MDRC Supp. at 13 (explaining that the copying of the work is merely "done in the process of extracting underlying unprotectable data").

[2652] *See* MDRC Supp. at 13 n.88.

[2653] *WIREdata*, 350 F.3d at 642-43.

[2654] *Id.* at 645; *see also Evolution, Inc. v. SunTrust Bank*, 342 F. Supp. 2d 943, 955-56 (D. Kan. 2004) (finding that copying portions of plaintiff's source code to extract defendants' own data from plaintiff's program was a fair use); *Nautical Solutions Marketing, Inc. v. Boats.com*, No. 8:02-CV-760-T-23TGW, 2004 WL 783121, at *2 (M.D. Fla. Apr. 1, 2004) (finding that temporarily copying public web pages in order extract unprotectable yacht listing facts was a fair use); *Ticketmaster Corp. v. Tickets.com, Inc.*, No. CV997654HLHVBKX, 2003 WL 21406289, at *2, *5 (C.D.Ca. Mar. 7, 2003) (finding that temporarily copying a competing ticket seller's website to extract unprotected public facts about events, such as dates, times, and prices, was a fair use).

[2655] *See* 2012 Recommendation at 74 (noting that noncommercial and personal uses may weigh in favor of fair use).

[2656] *Campbell*, 510 U.S. at 579 (explaining that the first factor looks to whether the new work "adds something new, with a further purpose or different character, altering the first with new expression, meaning, or message"); *Authors Guild, Inc. v. HathiTrust*, 755 F.3d 87, 97 (2d Cir. 2014) (finding that creating a full text searchable database from copied and digitized books was a transformative use).

In addressing the third factor, which considers the amount of the work used, proponents concede that in most cases the proposed use would involve reproduction of data outputs in their entirety.[2657] As the *WIREdata* case discussed above, courts have, however, been willing to permit complete copying of the original work in certain cases where it is necessary to achieve a permissible use.[2658] And in prior rulemakings, the Register has found such copying to be consistent with fair use, for example, in determining that the third factor is of little weight in the context of jailbreaking smartphones to enable interoperability, a salutary purpose. Here, the record suggests that copying of the data output in the form provided by the device manufacturer may be necessary to allow a patient to access and analyze the complete set of relevant data. Thus, even if the third factor arguably disfavors a fair use finding, the weight to be given to it under the circumstances is slight.[2659]

Factor four, regarding the effect on the market for or value of the copyrighted work, concerns "not only the extent of market harm caused by the particular actions of the [user], but also whether unrestricted and widespread conduct of the sort engaged in by the [proponent of fair use] . . . would result in a substantially adverse impact on the potential market."[2660] On the current record, there is no indication that the desired uses will usurp the market for medical devices, their corresponding monitoring systems, the copyrighted computer programs within those devices and systems, or the data outputs generated by those devices and systems.[2661] With respect to the devices and the software therein, as MDRC succinctly explains, "[n]o cardiac patient would look at a device's source code in lieu of getting a pacemaker; no patient with diabetes would look at the data readout from an insulin pump instead of getting one."[2662] Nor is there any indication in this record that home monitoring systems exist in a separate market from the medical devices themselves, or that a market exists for data outputs in and of themselves.

For their part, opponents provide no countervailing evidence of market harm or substitution for the devices, monitoring systems, software, or data outputs. To the extent that opponents assert that granting the exemption could erode the public's confidence in the safety and security of medical devices and potentially enable malicious hacking activities, the Register concludes that these harms are unsupported by record evidence

---

[2657] *See, e.g.*, Public Knowledge Class 27 Reply at 3-4.

[2658] *WIREdata*, 350 F.3d at 645 (holding that where the "only way [defendant] could obtain public-domain data about properties" was by "copying the compilation and not just the compiled data . . . it would be privileged to make such a copy"); *see also HathiTrust*, 755 F.3d at 98 ("For some purposes, it may be necessary to copy the entire copyrighted work, in which case Factor Three does not weigh against a finding of fair use."); *Kelly v. Arriba Soft Corp.*, 336 F.3d 811, 820-21 (9th Cir. 2003) (holding that the third fair use factor did not weigh against copier when copying the entire work was reasonably necessary).

[2659] 2010 Recommendation at 97; *see also* 2012 Recommendation at 73-74.

[2660] *Campbell*, 510 U.S. at 590 (internal quotations omitted).

[2661] *See, e.g.*, MDRC Supp. at 12, 23; MDRC Reply at 5; Public Knowledge Class 27 Reply at 3.

[2662] MDRC Reply at 5.

and therefore speculative in nature. In sum, the Register finds that, on the current record, the fourth fair use factor favors proponents.

On balance, based on the record in this proceeding, the Register finds that the proposed personal and noncommercial uses of patient data as described above are likely to be fair.

b. Adverse Effects

Proponents have successfully established that in many instances, access controls on medical device data outputs have, or are likely in the upcoming triennial period to have, an adverse impact on patients' ability to directly access their medical data.[2663] They have also established that TPMs are becoming more prevalent in the medical device industry, partly in response to FDA guidance on cybersecurity.[2664] The record further demonstrates that without an exemption, patients may be unable to see or analyze their data without visiting a hospital or doctor's office, and that there can be substantial benefits to allowing patients to access the data outputs as they are generated.[2665]

Although opponents urge that accessing data through health care providers is an acceptable alternative to circumvention,[2666] proponents convincingly explain that this alternative does not mitigate any adverse effects, because patients may have to wait months in order to receive vital information from their health care providers and may lose the opportunity to take corrective action in the meantime.[2667] Moreover, the record shows that even where a device or monitoring system provides some data to the patient, it may not provide other data that may help a patient manage or understand his or her own condition, as in the case of a continuous glucose monitor.[2668] Patients may thus be precluded from real-time monitoring of their own health status, including medical incidents reflected in data outputs, as well as the ability to correlate dietary practices and other behaviors with the impact on their physical well-being.[2669] The Register therefore concludes that, especially as they become increasingly prevalent, TPMs controlling access to medical device outputs are likely in the next three years to have an adverse effect on noninfringing uses of personal medical information.

[2663] *See* MDRC Supp. at 3, 18-19; MDRC Reply at 8-12.

[2664] *See* MDRC Supp. at 7, 9.

[2665] *See, e.g., id.* at App. C; Tr. at 8:01-06, 14:19-25, 15:10-18 (May 29, 2015) (West, MDRC).

[2666] AdvaMed Class 27 Opp'n at 2; NAM Opp'n at 5.

[2667] MDRC Reply at 9-10; Public Knowledge Class 27 Reply at 6.

[2668] *See, e.g.*, Tr. at 9:05-19 (May 29, 2015) (West, MDRC).

[2669] *See, e.g.*, MDRC Supp. at App. C.; Tr. at 7:21-8:09 (May 29, 2015) (West, MDRC).

c. Statutory Factors

The Register finds that the first factor, concerning the availability for use of copyrighted works,[2670] is essentially neutral or slightly favors proponents. Proponents persuasively establish that an exemption would not adversely affect the availability of works because patients would continue to obtain medical devices, the computer programs within those devices and data outputs generated by those devices, because such devices are necessary for the health of those patients.[2671]

Proponents do not directly address the second or third statutory factors. The Register finds that the second factor, concerning the availability for use of works for nonprofit archival, preservation, and educational purposes,[2672] does not appear especially relevant based on the record presented. With respect to the third factor, however, which addresses scholarship and research,[2673] the record shows that the exemption would permit personal research activities by virtue of patients' ability to access and analyze their medical data, as well as perhaps broader research and scholarly activities should patients choose to share that data with others.[2674] Factor three therefore weighs in favor of the exemption.

Regarding the fourth statutory factor,[2675] the Register determines that the effect of the exemption on the market for or value of the copyrighted works is unlikely to be adverse. As noted above, there is no indication in the record that the desired data access will usurp the market for medical devices, corresponding monitoring systems, or the computer programs within them.[2676] Furthermore, the record in this proceeding does not demonstrate the existence of a market for the data outputs generated by medical devices or monitoring systems. Factor four therefore also favors an exemption.

Finally, the statute also allows the Librarian to consider "such other factors" as may be appropriate.[2677] This "catchall" provision plays a significant role in the discussion and review of Proposed Class 27B. Opponents assert that the proposed exemption implicates significant health and safety concerns. These include potential dangers resulting from unauthorized circumvention, such as device malfunction, degradation, or even damage,[2678] as well as the efficacy and safety of medical devices if

[2670] 17 U.S.C. § 1201(a)(1)(C)(i).

[2671] *See* MDRC Supp. at 23.

[2672] 17 U.S.C. § 1201(a)(1)(C)(ii).

[2673] *Id.* § 1201(a)(1)(C)(iii)

[2674] *See* MDRC Supp. at 24, App. C; MDRC Reply at 12.

[2675] 17 U.S.C. § 1201(a)(1)(C)(iv).

[2676] *See* MDRC Supp. at 12 (citing *Cariou v. Prince*, 714 F.3d 694, 708-09 (2d Cir. 2013)); Public Knowledge Class 27 Reply at 3.

[2677] 17 U.S.C. § 1201(a)(1)(C)(v).

[2678] AdvaMed Class 27 Opp'n at 4.

they are subject to excessive data access requests.[2679] Opponents also urge that manufacturers who make and market medical devices must comply with a host of federal and state regulatory mandates, and that TPMs have played a role in ensuring such compliance.[2680] The serious nature of these concerns means that they must be carefully considered in evaluating Proposed Class 27B.

As suggested by some of the commenting parties, the Copyright Office advised FDA of the pendency of this proceeding, so that FDA could provide comments if it wished.[2681] In a communication to the Office, FDA expressed the overarching concern that allowing circumvention of TPMs on medical devices as a general matter could interfere with its regulatory authority over medical devices. This concern, however, would seem mainly to go to efforts to modify the devices themselves rather than passive access to patient data.[2682] As more pertinent here, FDA expressed wariness about facilitating access to data that includes patient health information or personally identifiable information, noting that the use of such data is regulated by agencies other than FDA.[2683] FDA therefore broadly recommended the Office clarify in any exemption that the exemption should not "affect the regulation of products that fall within the jurisdiction of other federal agencies."[2684]

The Register finds that, under the fifth statutory factor allowing for consideration of additional factors as appropriate, while the substantial issues of public safety, personal privacy, and regulatory compliance counsel caution, they do not necessarily weigh against an exemption. The proposal seeks to allow access to individual patient data for use by the patients themselves, not by third parties. It does not seek circumvention of software on medical devices themselves. In addition, as FDA suggests, an exemption can be crafted to ensure that privacy and other laws must be observed. On the whole, then, the statutory factors largely favor an exemption.

[2679] *Id.* at 2; LifeScience Alley Class 27 Opp'n at 4; NAM Opp'n at 7.

[2680] NAM Opp'n at 2; IPO Class 27 Opp'n at 3; LifeScience Alley Class 27 Opp'n at 2.

[2681] Letter from Jacqueline C. Charlesworth, Gen. Counsel and Assoc. Register of Copyrights, USCO, to Elizabeth H. Dickinson, Chief Counsel, FDA (May 12, 2015).

[2682] *See generally* Letter from Bakul Patel, Assoc. Dir. for Digital Health, Ctr. for Devices and Radiological Health, FDA, to Jacqueline C. Charlesworth, Gen. Counsel and Assoc. Register of Copyrights, USCO (Aug. 18, 2015) ("FDA Letter"). Consideration of FDA's response is appropriate because the matter of FDA's potential concerns with respect to this exemption has been part of the record since the filing of opposition comments on March 27, 2015. *See, e.g.*, AdvaMed Class 27 Opp'n at 3-4. This concern was also raised at the public hearings. *See* Tr. at 26:11-21 (May 29, 2015) (Sellars, MDRC). Proponents thus had the opportunity to address these concerns both in their reply comments and at the public hearings, and the record reflects significant public input on these issues in this class.

[2683] FDA Letter at 4-5 ("If [data] alludes to Patient Health Information (PHI), or Personal Identifiable Information (PII), then such information is regulated by other Federal Institutions and Agencies.").

[2684] *Id.* at 5.

4. NTIA Comments

NTIA recommends in favor of an exemption in Class 27B. Although NTIA notes that copying medical data "likely would not constitute an infringing activity," it nonetheless acknowledges opponents' claim that "a medical device's output could be entitled to copyright protection."[2685] Accordingly, like the Register, NTIA concludes that "in the event that the collection of medical data from a device does involve copying a protectable database structure, that copying is likely to be a fair use."[2686] NTIA explains that "granting an exemption would provide relief from the harm that proponents have demonstrated," namely, being "unable to see and react to data collected by medical devices (*e.g.*, glucose spikes, heart rate drops) in real time."[2687] NTIA also opines that the exemption is unlikely to adversely affect the operation of the medical device itself, relying on proponents' assertions that "some devices already continually collect data, and that one can intercept that data stream without interrogation, reducing or eliminating any additional strain on battery life."[2688]

NTIA acknowledges that "FDA has considerable regulatory authority in the area of medical device safety," and that "parties have raised important questions about safety and efficacy of medical devices."[2689] It thus proposes that the exemption language could provide as follows: "This exemption does not obviate the need to comply with other applicable laws and regulations, including any obligations that may arise under the Federal Food, Drug, and Cosmetic Act."[2690]

As discussed below, the Register agrees with NTIA that an exemption should be granted, that it should be limited to passive interception of data already generated by the device, and that it should expressly provide that actions taken under the exemption must be otherwise lawful.

5. Conclusion and Recommendation

At the outset, the Register observes that most would agree that patients should be able to access their own medical information. Traditionally, and continuing to today, much of that access is through medical professionals. But as technology evolves, it may offer new opportunities for individuals to monitor their own health and participate to a greater degree in their medical care. This exemption, in which patients seek to access the

[2685] NTIA Letter at 60-61.

[2686] *Id.* at 61

[2687] *Id.* at 59.

[2688] *Id.* at 60.

[2689] *Id.* at 62.

[2690] *Id.* While NTIA's proposed regulatory language states that the circumvention be permitted when conducted "at the direction of the patient," it does not address whether such a provision is consistent with the anti-trafficking provisions set forth in section 1201(a)(2) and (b). *See id.* at 61-62.

data generated by the sometimes life-saving medical devices upon which they rely, reflects just such a case.

Proponents have demonstrated that patient access to medical data generated by implanted medical devices and their corresponding personal monitoring systems is, and is likely to continue to be, hindered by TPMs that protect data outputs of those devices and systems. They have also established that, to the extent they involve copyrighted works, the uses in which proponents seek to engage are likely to be fair and noninfringing. Additionally, the statutory factors are supportive of an exemption, except for the potential safety and privacy concerns cited by FDA. Recognizing these concerns, while the Register recommends that an exemption be granted, the exemption should protect other agencies' regulatory authority, as detailed below.

As discussed above, a significant point of contention was the effect that circumvention might or might not have on the longevity or efficacy of devices due to requests for data outputs at a higher rate than what is normally transmitted. Although the record is somewhat inconclusive in this regard, what is clear is that proponents to some extent concede that battery life could be impacted by interrogation and have not demonstrated that the suggested harms will *not* occur from such activities. Accordingly, the Register will adopt the approach suggested by proponent MDRC, and recommend limiting the exemption to circumvention solely for the purpose of passively accessing data that is already being generated or transmitted by the device.

Further, as proposed by its supporters, the exemption would allow circumvention not only by a patient, but also "at the direction of a patient."[2691] While the Register is sympathetic to the practical issues that may arise if patients do not have the knowledge or the ability to circumvent TPMs, the phrase "at the direction of a patient" may implicate the anti-trafficking provisions set forth in section 1201(a)(2) and (b).[2692] Section 1201(a)(1) grants the Librarian the authority to adopt exemptions that apply to the prohibition on circumvention of technological measures that control access to copyrighted works, but does not grant authority to adopt exemptions concerning trafficking in circumvention tools. Moreover, section 1201(a)(1)(E) expressly provides that determinations made in the triennial rulemaking proceeding may not "be used as a defense in any action to enforce any provision of this title other than [the] paragraph [allowing for circumvention itself]."[2693]

A similar issue was present in the 2012 exemption for the unlocking of cellphones, which the Librarian granted in a manner consistent with section 1201(a)(1), expressly allowing circumvention initiated only by the owners of computer programs on

[2691] *See* MDRC Pet. at 1-2; NPRM, 79 Fed. Reg. at 73,871.

[2692] 17 U.S.C. § 1201(a)(2), (b). The anti-trafficking rules set forth in section 1201(a)(2) and (b) generally prohibit the manufacture and provision of technologies, products or services—or "part[s] thereof"—that are "primarily" designed for purposes of circumvention.

[2693] *Id.* § 1201(a)(1)(E); NOI, 79 Fed. Reg. at 55,688 n.2.

the phones.[2694] In order to broaden the exemption to allow circumvention "by another person at the direction of the owner," Congress enacted the Unlocking Consumer Choice and Wireless Competition Act[2695]—thus suggesting that it was necessary to amend the law to permit circumvention "at the direction of" an owner. [2696] Accordingly, the Register declines to recommend allowing circumvention "at the direction of a patient," and instead recommends, as consistent with section 1201(a)(1), circumvention only by the patient with respect to his or her own medical device or corresponding personal monitoring system.[2697] This limitation also helps to address some of the potential privacy issues raised by commenting parties and FDA.

Additionally, in light of the concerns expressed by opponents, as well as FDA, about the potential of any exemption to undermine other legal or regulatory mandates—including HIPAA, CFAA, or FDA regulations—any actions taken under the exemption will need to be compliant with all applicable laws and regulations. The Register notes that HIPAA provides important safeguards for individuals' medical records and other private medical information.[2698] The CFAA generally prohibits unauthorized access of computer systems.[2699] These laws and others, as well as FDA regulatory oversight, provide critical legal protections in relation to medical devices and their related computer systems and should be carefully studied by those seeking to take advantage of the exemption.

Although regulatory concerns expressed by FDA and other federal agencies have led the Register to recommend delaying the effective date of the exemptions for security research in Classes 25, 22, and 27A (except for voting machines), and for vehicle diagnosis, repair and modification in Class 21, the Register concludes that a delay of the exemption in this class is unnecessary. In the other classes, the agencies raised serious concerns about the effect of the exemptions on the health and safety of the public and on the environment that, based on the record, could not be fully addressed within the confines of this rulemaking process. Here, by contrast, these concerns do not appear as salient. While patient privacy is important, it is not apparent that the exemption would foster mishandling of data since it is being accessed by the patients to whom it belongs. Moreover, FDA does not express any specific health or safety concerns about the passive

---

[2694] 2012 Final Rule, 77 Fed. Reg. at 65,264. The 2010 exemption also included a similar limitation. 2010 Final Rule, 75 Fed. Reg. at 43,830-32.

[2695] Unlocking Act, Pub. L. No. 113-144, § 2(c), 128 Stat. 1751, 1751-52 (2014).

[2696] As discussed in Class 21, it may be useful for Congress to consider whether the accommodation provided in the Unlocking Act to allow assistance from third parties should be extended to circumvention activities beyond unlocking.

[2697] Even if the owner of a medical device is not the owner of the software, the Register finds that the uses encompassed by the exemption are likely to be fair.

[2698] 42 U.S.C. § 1320d-6; *see also The Privacy Rule*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule (last visited Oct. 7, 2015) (describing HIPAA privacy requirements).

[2699] *See* 18 U.S.C. § 1030.

monitoring of radio transmissions that are already being produced by a device or monitoring system, which is all that the exemption will allow.

Therefore, the Register recommends that the Librarian designate the following class:

> **Literary works consisting of compilations of data generated by medical devices that are wholly or partially implanted in the body or by their corresponding personal monitoring systems, where such circumvention is undertaken by a patient for the sole purpose of lawfully accessing the data generated by his or her own device or monitoring system and does not constitute a violation of applicable law, including without limitation the Health Insurance Portability and Accountability Act of 1996, the Computer Fraud and Abuse Act of 1986 or regulations of the Food and Drug Administration, and is accomplished through the passive monitoring of wireless transmissions that are already being produced by such device or monitoring system.**