



UNITED STATES DEPARTMENT OF COMMERCE
The Assistant Secretary for Communications
and Information
Washington, D.C. 20230

SEP 18 2015

Ms. Maria A. Pallante
Register of Copyrights
Library of Congress
James Madison Memorial Building
Washington, DC 20540-3120

Re: Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. 2014-07

Dear Ms. Pallante:

As Assistant Secretary for Communications and Information and Administrator of the National Telecommunications and Information Administration (NTIA), an agency of the U.S. Department of Commerce, I am pleased to submit our views on proposed exemptions from the Digital Millennium Copyright Act's (DMCA) prohibition against circumvention, as required by Title 17, Section 1201(a)(1)(C) of the United States Code.¹ NTIA appreciates the opportunity to offer its unique perspective and expertise as part of this process. As mandated by Congress, NTIA promotes "the benefits of technological development in the United States for all users of telecommunications and information facilities,"² and serves "as the President's principal adviser on telecommunications policies pertaining to the Nation's economic and technological advancement."³

As in previous rulemakings, our input to you reflects our core mission to advance the President's goal of promoting the free flow of information over a ubiquitous, open, and affordable Internet.⁴ We believe the potential of information technology is maximized in part when the legal environment simultaneously protects intellectual property rights, facilitates a competitive marketplace, and enables all Americans to exercise their right to make noninfringing use of lawfully-obtained works.

NTIA has conducted an extensive review and analysis of the record in this rulemaking, and has prepared detailed recommendations rooted in our subject matter expertise as well as in statute. We have organized our recommendations in a fashion that enables us, as much as

¹ 17 U.S.C. § 1201(a)(1)(C) sets forth the required consultative process, which is that "during each succeeding 3-year period, the Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation, shall make the determination in a rulemaking proceeding..."

² 47 U.S.C. § 901(c)(1) (2012).

³ 47 U.S.C. § 901(b)(2)(D) (2012).

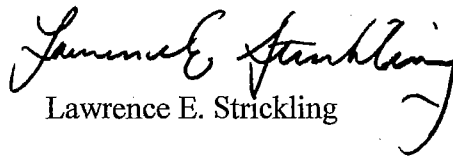
⁴ The Department of Commerce has declared the following core policy in its work regarding the Internet: "Recognizing the vital importance of the Internet to U.S. prosperity, education, and political and cultural life, the Department has made it a top priority to ensure that the Internet remains open for innovation." *Inquiry on Copyright Policy, Creativity, and Innovation in the Internet Economy*, Docket No. 100910448-0448-01, Notice of Inquiry, 75 Fed. Reg. 61,419 (Oct. 5, 2010).

possible, to avoid repeating similar discussions in separate classes. The attached document presents NTIA's views on each of the proposed exemptions, and provides some broader observations about both the process and substance of the rulemaking.

We appreciate the opportunity to express our views to you on the important questions raised in this proceeding. Past exemptions recommended by your office have in many cases provided a foundation for innovation and economic growth in our country, and we look forward to continuing to work with you to pursue those goals.

Should you have any questions regarding this discussion, please feel free to call me at 202-482-1840. Thank you again for your consideration of NTIA's views on this important matter.

Sincerely,

A handwritten signature in cursive script, reading "Lawrence E. Strickling". The signature is written in dark ink and is positioned above the printed name.

Lawrence E. Strickling

Attachment

SIXTH TRIENNIAL SECTION 1201 RULEMAKING

**RECOMMENDATIONS OF THE NATIONAL
TELECOMMUNICATIONS AND INFORMATION
ADMINISTRATION TO THE REGISTER OF COPYRIGHTS**



SEPTEMBER 18, 2015

Table of Contents

Recommendations	3
I. Broad Observations	3
A. Enhancements to the Rulemaking Process	3
B. Treatment of Non-Copyright Policy Issues	3
C. Use of Access Controls for Non-Copyright Purposes	6
D. Similar Works on Different Devices	8
II. Specific Classes	10
A. Audiovisual Works	10
1. Educational Uses (Classes 1-4)	11
2. Filmmaking and Other Derivative Work Creation (Classes 5-7)	23
3. Space Shifting and Format Shifting (Class 8)	29
B. Literary Works Generally	33
1. Interoperability with Assistive Technologies (Class 9)	33
2. Space Shifting and Format Shifting (Class 10)	35
C. Unlocking: Software Interoperability with Networks (Classes 11-15)	36
D. Jailbreaking: Software Interoperability with Software	42
1. Mobile Devices (Classes 16-18)	42
2. Video Game Consoles (Class 19)	46
3. Smart Televisions (Class 20)	49
E. Data Access, and Diagnosis, Repair, or Modification of Software-Driven Devices	52
1. Motorized Land Vehicles (Class 21)	52
2. Medical Devices (Part of Class 27)	59
F. Using Unsupported Software	64
1. Video Games (Class 23)	64
2. Music Recording Software (Class 24)	70
G. Software Security and Safety Research (Classes 22, 25, Part of 27)	71
H. 3D Printer Software Interoperability with Feedstock (Class 26)	89

Recommendations

The National Telecommunications and Information Administration (NTIA), an agency of the U.S. Department of Commerce, respectfully submits the following recommendations as part of the statutorily-required consultative process pursuant to Title 17, Section 1201(a)(1)(C) of the United States Code.

I. Broad Observations

Prior to our discussion of specific proposed exemptions, NTIA offers four general observations related to this rulemaking:

A. Enhancements to the Rulemaking Process

NTIA applauds the Copyright Office for implementing constructive process changes for the sixth triennial rulemaking under Section 1201. First, NTIA thanks the Office for the opportunity to ask questions during the hearings. We appreciate being included in this fashion and hope the questions we asked served to further clarify the record. Additionally, procedural innovations such as enabling members of the public to submit initial petitions without “requiring the proponent of an exemption to deliver the complete legal and evidentiary basis for its proposal with its initial submission,”¹ and providing prospective submitters with petition templates, were helpful to interested parties who lacked previous experience with the rulemaking process. Similarly, the three-round public comment phase and requirement that each comment submission address one specific proposed exemption facilitated the development of a clear and comprehensive record. NTIA also appreciates the Office’s continued practice of posting the entire record, including multimedia evidence and hearing exhibits, online for public inspection.

We recommend preserving and building on these process improvements in future rulemakings. NTIA remains concerned about the accessibility of these proceedings to members of the public who lack expertise in copyright law or the resources to retain counsel, yet may be adversely affected by either the prohibition against circumvention or proposed exemptions from the prohibition. We also remain concerned that the process can be inefficient and problematic for petitioners seeking exemptions that have been previously granted. NTIA would welcome the opportunity to discuss possible further enhancements to the rulemaking process once this proceeding is complete.

B. Treatment of Non-Copyright Policy Issues

While there have long been proposed exemptions that implicated issues unrelated to copyright law,² the sixth triennial rulemaking has stood out for its extensive discussions of

¹ Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. 2014-07, Notice of Inquiry and Request for Petitions, 79 Fed. Reg. 55,687, 55,692 (Sept. 17, 2014) (*2014 Notice of Inquiry*).

² For example, while unlocking mobile phones may require circumvention of a technological protection measure (TPM) under Section 1201, and while past proceedings on the topic have included discussion of copyrighted works,

matters with no or at best a very tenuous nexus to copyright protection.³ Parties have, in this proceeding, raised concerns about medical device safety, vehicle emissions standards, best practices in software vulnerability disclosure, and other issues that are not contemplated in copyright law.⁴ In asserting the relevance of such matters to this proceeding, parties often cite the fifth statutory factor in this rulemaking, which allows the Librarian of Congress (and by extension, the Copyright Office) to consider “such other factors as the Librarian considers appropriate.”⁵

NTIA urges the Copyright Office against interpreting the statute in a way that would require it to develop expertise in every area of policy that participants may cite on the record. Although Congress clearly included this factor to enable consideration of issues not otherwise enumerated, the deliberative process should not deviate too far afield from copyright policy concerns.⁶ As the Register of Copyrights noted in 2010, “the focus in this rulemaking is limited to actual or likely adverse effects on noninfringing uses of copyrighted works. No other agency has delegated authority to temporarily limit the application of the prohibition on circumvention. This

the practice and its restriction primarily implicate competition and marketing policies, rather than copyright interests. During the rulemaking that ended in 2006, proponents of the first unlocking exemption argued that “the circumventor access[es] the firmware merely to reprogram it to work on a different network, or to utilize a different SIM card,” and is not “exercising any exclusive right the copyright owner has in the mobile firmware.” *Comments of The Wireless Alliance* at 2, Docket No. 2005-11, available at http://www.copyright.gov/1201/2006/comments/granick_wirelessalliance.pdf. NTIA explained the importance of unlocking to telecommunications policy in a 2013 petition for rulemaking to the Federal Communications Commission. *See Petition for Rulemaking of the National Telecommunications and Information Administration* (Sept. 17, 2013), available at http://www.ntia.doc.gov/files/ntia/publications/ntia_mobile_devices_unlocking_petition_09172013.pdf.

³ For example, in opposing an exemption for using third party feedstock with 3D printers, Stratasys states that it “spent millions of dollars and years certifying this plastic to be on a commercial airplane for 25 years to get the FAA to approve it.” As a result, the company’s customers in the aircraft industry “don’t want anybody to be able to get into that integrated system.” Transcript of May 28, 2015, Hearing on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Section 1201 – Digital Millennium Copyright Act (*May 28 Hearing Transcript*) at 101-02, Docket No. 2014-07, available at <http://copyright.gov/1201/2015/hearing-transcripts/1201-Rulemaking-Public-Roundtable-05-28-2015.pdf>.

⁴ There have been many discussions in this proceeding that are largely devoid of copyright-related matters. In its comments opposing an exemption for security research, for example, BSA mainly argues that “the proposal would in fact authorize the public disclosure of security vulnerabilities in ways that would expose the public to heightened security risks.” Regarding the implications for copyright, BSA states only that “the proponents seek to engage in such a wide variety of activities that it is impossible to assess whether all of these activities qualify as noninfringing,” and asserts that proponents have not provided sufficient evidence of harm from the prohibition against circumvention. *See Class 25 Comments of the Business Software Alliance (BSA Class 25 Comments)* at 2, 5, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%2025/BSA_The_Software_Alliance_Class25_1201_2014.pdf.

⁵ 17 U.S.C. § 1201(a)(1)(C)(v) (2012).

⁶ Indeed, the DMCA Conference Report noted that “it is the intention of the conferees that ... *in recognition of the expertise of the Copyright Office*, the Register of Copyrights will conduct the rulemaking” in its entirety, up to “recommending final regulations in the report to the Librarian.” H.R. REP. NO. 105-796, at 64 (1998) (Conf. Rep.) (emphasis added).

prohibition was established to provide legal support for, and foster the availability of, copyrighted works in the digital environment.”⁷ Therefore, the Office should not, in its deliberations, heavily weigh unrelated matters such as greenhouse gas emissions or the quality of materials used to build aircraft, and should instead focus primarily on questions relevant to copyright law.⁸ Congress, applicable regulatory agencies, and their counterparts within state governments are well-equipped to deal with these non-copyright issues in the appropriate settings and under legal authorities focused on those issues.⁹

Despite NTIA’s views on the treatment of non-copyright policy issues in this proceeding, NTIA recognizes that the Copyright Office may understandably be apprehensive about recommending exemptions that could inadvertently implicate issues of safety and security. One possible way forward may be to delay the date upon which such an exemption would become effective to allow the relevant stakeholders in other policy spheres to prepare for the exemption’s effective date. NTIA is not convinced such a delay would be helpful, and urges the Copyright Office to keep any delay as short as practicable. If the Copyright Office were persuaded that an exemption is warranted because proponents have sufficiently demonstrated the adverse effects of access controls on noninfringing use of the underlying works, a delay would prolong that demonstrated harm and not provide the immediate relief that proponents seek and the statute contemplates.¹⁰ In addition, any significant delay to an exemption would cause various problems for the next rulemaking.¹¹ Deviation from the statutory triennial schedule may cause confusion in the marketplace;¹² adhering to the contemplated timeline of this rulemaking would provide

⁷ Recommendation of the Register of Copyrights (*2010 Register of Copyrights Recommendation*) at 103, Docket No. RM 2008-8, (June 11, 2010), available at <http://www.copyright.gov/1201/2010/initialed-registers-recommendation-june-11-2010.pdf>.

⁸ NTIA acknowledges that when analyzing the adverse effects of granting or not granting an exemption, the factors analyzed will not always be strictly related to copyright law. However, our concern is that non-copyright issues seemed to consume the majority of the current proceeding; giving the fifth statutory factor this much weight appears contrary to Congressional intent.

⁹ For example, the Computer Fraud and Abuse Act (CFAA), the Federal Food, Drug, and Cosmetic Act administered by the Food and Drug Administration (FDA), the Clean Air Act administered by the Environmental Protection Agency (EPA), the National Traffic and Motor Vehicle Safety Act administered by the National Highway Traffic Safety Administration, and their state equivalents may all be relevant venues for these issues.

¹⁰ NTIA uses the terms “access control” and “technological protection measure” (TPM) to refer to a “technological measure that effectively controls access to a work protected under [the Copyright Act]” as set forth in 17 U.S.C. § 1201(a). Both terms will be used interchangeably throughout this recommendation.

¹¹ This proceeding is conducted every three years, but proponents for exemptions must petition for them a year in advance to allow for time to prepare. The Notice of Inquiry and Request for Petitions for this rulemaking was published on September 17, 2014, and the Notice of Proposed Rulemaking was published in the Federal Register on December 12, 2014, but the exemption decisions will not be published until October 2015. If the delay were more than a few months, enough time will not have passed for either the interested parties or the Copyright Office to determine whether the exemption had any effect on the demonstrated harms, and whether the exemption itself caused any harms.

¹² The Librarian issued a time-limited exemption at the end of the 2012 rulemaking, when he exempted circumvention for the purpose of unlocking mobile handsets originally sold no later than January 26, 2013. *See*

consistency to the benefit of consumers and users of the exemptions. Moreover, it is unclear whether the legislative history supports delaying the effective date of an exemption.¹³ In sum, NTIA is cognizant that there may be concerns whenever an exemption is granted for the first time, but after several rulemakings under section 1201 of the DMCA, there is no evidence that a particular exemption has caused substantial damage or halted the market for particular works, or had ancillary harmful impacts outside of the copyright space.

C. Use of Access Controls for Non-Copyright Purposes

NTIA is pleased that manufacturers of electronic devices and other stakeholders are increasingly focused on securing sensitive data and protecting the integrity of their software.¹⁴ Encryption and other security measures are critical tools for building more trustworthy systems, particularly when devices store and transmit personal and sensitive information. Accordingly, regulatory authorities such as the Food and Drug Administration have called on industry to include security measures in their products.¹⁵

Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. 2011-07, *Final Rule*, 77 Fed. Reg. 65,260, 65,264-66 (Oct. 26, 2012) (*2012 Final Rule*), available at <http://copyright.gov/fedreg/2012/77fr65260.pdf> (Issuing an unlocking exemption for handsets “originally acquired from the operator of a wireless telecommunications network or retailer no later than ninety days after the effective date of this exemption.”). This decision led to considerable public confusion. In its coverage of the decision, *The New York Times* reported that the unlocking exemption “expires [on January 26th, 2013], making the act of unlocking a cellphone potentially illegal, unless it is authorized by a carrier.” See Chen, Brian X., *A Right to Unlock Cellphones Fades Away*, *The New York Times* (Bits blog), (Jan. 25, 2013), available at <http://bits.blogs.nytimes.com/2013/01/25/cellphone-unlock-dmca/>.

¹³ NTIA could not find any discussion in the legislative history to support delaying the effective date of an exemption but the House Manager’s Report states that “a determination that the exceptions in Section 1201(a)(1) are in effect for a particular class of works means that enforcement against someone who circumvents a technological measure that effectively controls access to a work falling in that class may not be undertaken during the period (not to exceed three years) covered by the determination.” See Section-by-Section Analysis of H.R. 2281 As Passed By the United States House of Representative on August 8, 1998, Committee on the Judiciary, House of Rep., 105th Cong., 2d Sess. 8 (Comm. Print, Serial No. 6, Sept. 1998). The “period covered by the determination” may be interpreted to mean the period at issue in a rulemaking as a whole, rather than a time period contemplated for a particular proposed class.

¹⁴ See, e.g., Russell L. Jones, & Sheryl Coughlin, *Networked medical device cybersecurity and patient safety: Perspectives of healthcare information cybersecurity executives*, Deloitte Issue Brief (2013), available at <http://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lhsc-networked-medical-device.pdf>; see also Andrea Peterson, *Connected medical devices: the Internet of things-that-could-kill-you*, Washington Post – The Switch (Aug. 3, 2015), <https://www.washingtonpost.com/news/the-switch/wp/2015/08/03/connected-medical-devices-the-internet-of-things-that-could-kill-you/>; Sue Poremba, *Cyber Security is Growing in Importance for Medical Devices Too*, Forbes Business (Jan. 19, 2015), <http://www.forbes.com/sites/sungardas/2015/01/19/cyber-security-is-growing-in-importance-for-medical-devices-too/>; John D. Halamka, MD, *The Security of Medical Devices*, Life as a Healthcare CIO (Aug. 5, 2015), <http://geekdoctor.blogspot.com/2015/08/the-security-of-medical-devices.html> (discussing recent cybersecurity threats and the measures that stakeholders and device manufacturers are taking to address them).

¹⁵ See U.S. Food and Drug Administration, *Medical Devices – Cybersecurity* (Oct. 23, 2014), available at <http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/ucm373213.htm>.

NTIA is concerned, however, that security measures that have been deployed for non-copyright reasons—such as security and privacy, or possibly anti-competitive goals—are being described in this rulemaking as technological measures controlling access to copyrighted works under Section 1201.¹⁶ This is a fundamental misuse of Section 1201, which can lead to reduced respect for the DMCA and copyright law, and can yield either an inappropriate overprotection of copyright (out of concern, for example, to avoid harming security), or a reduction in security (because of a grant of an exemption in this proceeding where indeed no significant copyright interest is at issue).

A related problem would arise if a manufacturer were to use the same technological protection measure to achieve two functions—enhance security and protect a legitimate copyright interest. Again, this could lead to inappropriate outcomes, and manufacturers would in many cases be well advised to separate techniques aimed at copyright protection from those aimed at security and privacy.

These concerns lead to two practical considerations. First, a record showing that a technological measure was not deployed with copyright protection in mind should weigh heavily in favor of a proposed exemption. Such a standard is entirely consistent with the statutory factors to be considered in this rulemaking.¹⁷

Second, the increasing ubiquity of security measures has led to a widespread assumption that Section 1201 applies in a broader set of circumstances than may, in reality, be true. One of the clearest examples of this phenomenon appeared during the previous triennial rulemaking, when one group of proponents sought an exemption for circumventing access controls protecting public domain works.¹⁸ The problem has further manifested itself during this proceeding, as

¹⁶ For example, General Motors devotes a section of its comments on Class 21 to “the purpose of TPMs in the modern car.” The company does not mention protection of copyrighted works as a reason for implementing these access controls, instead stating that auto makers “employ TPMs in vehicles to help protect them from tampering and hacking.” General Motors further argues that “with TPMs as part of systems protecting vehicle safety, regulatory compliance, and a subsequent owner’s trust in the integrity of vehicle systems, it would be inappropriate to permit their circumvention.” See Class 21 Comments of General Motors (*GM Class 21 Comments*) at 4-5, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%2021/General_Motors_Class21_1201_2014.pdf.

¹⁷ For example, factor (iv) directs the Librarian to consider “the effect of circumvention of technological measures on the market for or value of copyrighted works.” 17 U.S.C. § 1201(a)(1)(C)(iv) (2012). If a copyright holder does not implement an access control to protect the underlying work, then it may be difficult to articulate how circumvention of said access control would negatively impact the value of the work. This view is consistent with the view expressed by the Register in 2006 with respect to mobile phone unlocking: “The purpose of the software lock appears to be limited to restricting the owner’s use of the mobile handset to support a business model, rather than to protect access to a copyrighted work itself.... The Register’s recommendation is based on law and policy considerations relating to 17 U.S.C. § 1201(a)(1) and on her conclusion that the record relating to this proposed class of works does not demonstrate any copyright-based rationale for enforcing the prohibition on circumvention of technological measures that control access to works protected by copyright.” Recommendation of the Register of Copyrights (2006 *Register of Copyrights Recommendation*) at 51 n. 148, Docket No. RM 2005-11, (Nov. 17, 2006), available at http://www.copyright.gov/1201/docs/1201_recommendation.pdf.

highlighted by the confusion over whether circumvention is necessary to make certain repairs to video game consoles,¹⁹ as well as the possibility that the *Lexmark* decision²⁰ may have placed some acts of circumvention involving 3D printers outside the scope of Section 1201.²¹ In these circumstances, the Copyright Office has a role to play in clarifying the scope of Section 1201 through these proceedings. Where the prohibition against circumvention clearly does not apply, NTIA recommends the Copyright Office continue its previous practice of noting that a “requested exemption is beyond the scope of this rulemaking proceeding.”²² Similarly, in cases where the prohibition may apply, but only in certain instances, NTIA suggests noting the prohibition’s limitations when recommending an exemption to the Librarian. NTIA further encourages the Copyright Office to make clear to manufacturers and content creators that they should remain cognizant of the underlying purposes for which an access control is implemented. Manufacturers should not implement access controls on devices to restrict certain device functions or enforce non-copyright-related business models—which is not the purpose behind Section 1201—and then try to use the DMCA to enforce a business model or limit a user’s post-purchase modification of a device.

D. Similar Works on Different Devices

The sixth triennial rulemaking is also noteworthy for the wide range of electronic devices that contain essentially identical works, accompanied by separate requests to circumvent access controls on those works for very similar purposes. This is a natural consequence of current trends in computing technology, where modular equipment and computer programs are adapted for different purposes; one witness demonstrated this effectively and convincingly, during the May 21st hearing, by laying out a wide array of devices on a table—ranging in size from an Apple Watch to an iPad—and noting that they all run variations on the same operating system.²³ The

¹⁸ Comments of the Open Book Alliance, Docket No. RM 2011-07 (Dec. 1, 2011), *available at* http://www.copyright.gov/1201/2011/initial/open_book_alliance.pdf.

¹⁹ See Transcript of May 20, 2015, Hearing on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Section 1201 – Digital Millennium Copyright Act (*May 20 Hearing Transcript*) at 304-310, Docket No. 2014-07, *available at* <http://copyright.gov/1201/2015/hearing-transcripts/1201-Rulemaking-Public-Roundtable-05-20-2015.pdf> (capturing a discussion between iFixit and ESA representatives regarding whether iFixit’s desired repairs require circumvention of TPMs).

²⁰ See *Lexmark Int’l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522 (6th Cir. 2004).

²¹ See Class 26 Comments of Public Knowledge and the Library Copyright Alliance (*Public Knowledge Class 26 Comments*) at 6-8, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_longform_PK_and_LCA_Class26.pdf.

²² Recommendation of the Register of Copyrights (2012 *Register of Copyrights Recommendation*) at 15, Docket No. 2011-07, (Oct. 12, 2012), *available at* http://www.copyright.gov/1201/2012/Section_1201_Rulemaking_2012_Recommendation.pdf.

²³ See Transcript of May 21, 2015, Hearing on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Section 1201 – Digital Millennium Copyright Act (*May 21 Hearing Transcript*) at 58-61, Docket No. 2014-07, *available at* <http://copyright.gov/1201/2015/hearing-transcripts/1201->

Android operating system is similarly found in a range of devices. Nevertheless, adhering to precedent set during previous rulemakings, portions of the record in this proceeding are dominated by discussions of which specific types of devices should be included in proposed exemptions, particularly those related to network interoperability (“unlocking”)²⁴ and software interoperability (“jailbreaking”).²⁵

Because the range of computing devices continues to expand, NTIA believes that, moving forward, it would be more appropriate to focus on the class of work that proponents seek to circumvent (e.g., mobile operating systems), rather than considering separate exemptions for each type of device where such works are found. The current approach of attempting to distinguish among devices is not well suited for future rulemakings. Whether to call a software-driven device a phone, a tablet, or a watch is largely a marketing distinction. As noted earlier and, as demonstrated by the record, many of these devices are able to run the same operating systems and provide identical or nearly identical functionalities using those works.

Thus, a more practical and efficient way to ensure that consumers are adequately protected from any harm caused by the prohibition against circumvention is to avoid unnecessarily constraining exempted classes based on the specific types of devices on which works are contained. When multiple types of computing devices are distributed with substantially similar works and technological measures protecting those works, there should be no need to require that proponents provide a full evidentiary record for each device, nor must the Copyright Office enumerate specific types of devices in an exemption. This approach is consistent with the Register’s prior conclusion that “a ‘particular class of copyrighted works’ must relate primarily to attributes of the copyrighted works themselves and not to factors that are external to the works, e.g., the material objects on which they are fixed or the particular technology employed on the works.”²⁶ While the particular type of device in question may in some instances be an appropriate vehicle for narrowing exemption language to fit the record, such a restriction is of questionable utility when the copyrighted works at issue are substantially similar across devices. When exemptions distinguish among specific devices, consumers are left confused and wondering why an exemption covers one particular device but not a slightly smaller or larger one, even though they operate in relatively similar fashion. Therefore, the focus in this

[Rulemaking-Public-Roundtable-05-21-2015.pdf](#); see also Exhibit 8 for Proposed Classes 16-18, Hearing Exhibits, Hearing on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Section 1201 – Digital Millennium Copyright Act, Docket No. 2014-07, available at http://copyright.gov/1201/2015/hearing-exhibits/IMG_0041.JPG (illustrating the similarity in design and operation across the spectrum of Apple mobile devices).

²⁴ See Exemption to Prohibition on Circumventing Access Control Technologies, *Notice of Proposed Rulemaking*, 79 Fed. Reg. 73,856, 73,863-66 (Dec. 12, 2014) (2014 NPRM) available at <http://copyright.gov/fedreg/2014/79fr73856.pdf>.

²⁵ See *id.* at 73,866-68.

²⁶ Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. RM 99-7D, *Final Rule*, 65 Fed. Reg. 64,555, 64,562 (Oct. 27, 2000) (2000 *Final Rule*), available at <http://www.copyright.gov/fedreg/2000/65fr64555.pdf>.

proceeding should be on the need to circumvent—and potential harm from circumventing—access controls protecting the copyrighted works at issue, rather than the size of the screen or other details of the devices on which the works are contained.²⁷ Crafting exemptions based on classes of works rather than devices would, in many ways, eliminate the large effort of determining which devices should be included, and would more appropriately align with the original purpose of this rulemaking.

II. Specific Classes

NTIA submits the following recommendations on the specific classes addressed in petitions to the Copyright Office.

A. Audiovisual Works

Proposed classes one through eight exemplify the purpose of Section 1201, which is to deter copyright infringement in the digital age while allowing for lawful uses of copyrighted works.²⁸ NTIA acknowledges the concerns raised by rights holders who oppose broad exemptions that cover their works, but emphasizes that exemptions issued under the statute are unable to legalize copyright infringement. The record does not show that previous grants of similar exemptions have led to an increase in infringement, but rather that educators, students, filmmakers, and authors have used them in accordance with fair use principles to create new and transformative works.²⁹

²⁷ For example, one analytical tool could be to consider a computer operating system as a protected work. Under this approach, devices of any physical size that run that operating system would fall within the scope of an exemption encompassing that work.

²⁸ See, e.g., Class 2 Comments of Renee Hobbs, et al. (*Hobbs Class 2 Comments*) at 2, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments020615/InitialComments_LongForm_Hobbs_Class02.pdf. (“The spirit of the Section 1201 rulemaking process is to protect and preserve fair use in the digital age.”).

²⁹ See, e.g. Class 1 Comments of Peter Decherney, et al. (*Decherney Class 1 Comments*) at 2, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments020615/InitialComments_LongForm_DecherneyEtAl_Class01.pdf; (“Technological protection measures and exemptions for education have coexisted peacefully for year. The explosive growth in the availability of motion picture to consumers has happened alongside modest and incremental growth in an exemption for education users.”); Class 1 Comments of Jeremy N. Sheff at 1, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_Sheff_Class01.pdf (“Since the enactment of this exemption, I have also taken advantage of the exemption to embed a clip from another copyrighted audiovisual work in a slideshow presentation on property law theory for my property law class. In this class session, I use a short video clip from authorized copy of a popular children’s television show to demonstrate how moral intuitions regarding ownership rights are culturally embedded from a very early age, and to hold those intuitions up for critical analysis. Having a high-quality clip to demonstrate this point without having to switch presentation media or technology platforms allows for the discussion of these issues to flow smoothly and contributes to effective presentation of the relevant concepts.”); *Hobbs Class 2 Comments* at 4 (citing a teacher who due to the exemption was able to combine clips of adaptations of Shakespeare’s works into a single DVD with all necessary clips for the unit in order to show how Shakespeare’s worked are used, referenced or acknowledged in popular culture and other works of literature and art.); Class 6 Comments of the International Documentary Association, et al. at 13 (*IDA Class 6 Comments*), Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments020615/InitialComments_LongForm_IDA_Class06.pdf (“[T]he documentary *Inequality for All* relied on

Proponents seek the ability to circumvent TPMs employed to protect audiovisual works embodied in physical media, as well as audiovisual works obtained through online download and streaming services.³⁰ The TPMs include but are not limited to the Content Scramble System (CSS) on DVDs, the Advanced Access Content System (AACS) utilized on Blu-ray discs, and the variety of access controls that protect audiovisual works distributed over the Internet, such as Protected Streaming, Microsoft PlayReady, and Apple's FairPlay.³¹

NTIA has divided the eight proposed classes of audiovisual works into three general categories—(I) educational uses, (II) filmmaking and other derivative work creation, and (III) space shifting and format shifting.³²

1. Educational Uses (Classes 1-4)

Four proposals seek to renew and expand current exemptions for educational uses of audiovisual works. The proposed exemptions for audiovisual works for educational uses are: educational uses by university and college students and faculty, educational uses by K-12 students and teachers, educational uses in Massive Open Online Courses (MOOCs) by instructors and students, and educational uses in libraries, museums, and non-profit organizations.³³ Two of the proposed exemptions, covering university and K-12 educational

the fair use exemption for documentary films to show an interview with the president of Viacom, Inc. that painted the president in a bad light. The filmmakers attempted to license the clip, but were given a no-explanation turndown letter. Without fair use and the proposed exemption, they would have been unable to use the footage.”); Class 7 Comments of New Media Rights (*NMR Class 7 Comments*) at 4, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_NewMediaRights_Class06.pdf (“Anita Sarkeesian... creates and produces Feminist Frequency, an online web series that analyze popular culture from a feminist perspective.... [Her] work relies heavily on access to video clips from DVDs. Her remix videos convey educational messages to the public and critique contemporary society [.]”).

³⁰ See Initial Petition of Decherney, et al. (*Decherney Petition*) at 1-2, Docket No. 2014-07, available at http://copyright.gov/1201/2014/petitions/Decherney-et-al_1201_Initial_Submission_2014.pdf.

³¹ *Id.* at 3.

³² Educational uses include Classes 1-4. Filmmaking and other derivative work creation includes Classes 5-7. Space shifting and format shifting includes Class 8. *2014 NPRM* at 73,859-63.

³³ Importantly, NTIA is using the term “instructors,” “educators” and “faculty” interchangeably to help eliminate possible confusion as to who may qualify for these exemptions. Previously the term “professors” has been utilized as a defining term for university and college educators for which the proposed exemption will apply. However, this term is potentially too limiting as not all instructors at the university level are given the title of professor. Many are adjunct, term, part time, teaching assistants or other staff or faculty. NTIA intends that all instructors and faculty qualify for these exemptions. See, e.g. *Decherney Class 1 Comments* at 4-5 (He uses the terms faculty, staff, professors, teaching assistants and educators throughout the description of this particular proposed exemption demonstrating that his intent is to not limit it to one small subset of educators). Further, this exemption will not always be used in the classroom, but may be used as a part of research that will lead to classroom instruction. These types of uses should not be precluded from this exemption and therefore should be included in the term “faculty.” See Class 1 Comments of the Music Library Association at 1, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_MLA_Class01.pdf (MLA also uses the terms librarians, scholars and researchers in defining the term faculty).

settings, are based on existing exemptions. NTIA supports the renewal of these existing exemptions as well as expansion in several respects, including to cover works distributed on Blu-ray discs. The current record for Blu-ray is more substantial than in the 2012 proceeding.³⁴ As high definition formats become the norm, an exemption that includes Blu-ray—in addition to DVD- and Internet-distributed content—is justified.³⁵

The other two proposed classes are new to this rulemaking. The first one seeks the ability to circumvent access controls on works for students and educators in “Massive Open Online Courses” or MOOCs.³⁶ These courses are different from traditionally offered online college courses because they are available via the Internet to anyone, and are found outside formal educational settings.³⁷ The second new proposal would allow circumvention of access controls by educators and learners in programs conducted by museums, libraries, and non-profit organizations.³⁸ Proponents of these two classes have intentionally requested broad language that would allow for a growing number of unconventional learning environments to take advantage of an exemption in order to promote digital literacy.³⁹

Having analyzed the record, NTIA recommends granting all requested exemptions for these classes of works with modified language that will be described below. Opponents did not present evidence that the existing exemptions have enabled copyright infringement since the Copyright Office began recommending this type of exemption over the past several rulemakings, and indeed they generally did not object to renewal of the existing exemptions.⁴⁰ Consequently, the

³⁴ See, e.g., Class 3 Comments of Peter Decherney, et al. (*Decherney Class 3 Comments*), Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_DecherneyEtAl_Class03.pdf (describing the unique benefits that high definition content offers for students and teachers of MOOCs).

³⁵ In the comments, proponents cited works available through subscription-based streaming services such as Netflix and Amazon Prime. See *Decherney Class 1 Comments* at 17. However, for the purposes of this exemption, the classification “works acquired via online distribution” does not include works streamed via a subscription-based service where the user is not an owner of the copy of the work. However, a digital download copy that accompanies the purchase of a DVD or Blu-Ray would qualify for circumvention under this exemption.

³⁶ See generally *Decherney Class 3 Comments*.

³⁷ *Id.* at 2.

³⁸ See Class 4 Comments of Renee Hobbs (*Hobbs Class 4 Comments*), Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_HobbsEtAl_Class04.pdf

³⁹ See *Decherney Class 3 Comments* at 6 (“It would artificially constrain the growth and evolution of MOOCs to limit the definition in any of the ways [suggested by the Copyright Office in the Notice for Proposed Rulemaking].”); Class 4 Reply Comments of Renee Hobbs, et al. (*Hobbs Class 4 Reply Comments*) at 4-5, Docket No. 2014-07, available at http://copyright.gov/1201/2015/reply-comments-050115/class%204/ReplyComments_LongForm_Hobbs_Class04.pdf (“Teaching and learning is a highly variable practice; situational variation is necessary for education to be responsive to the specific contexts of informal education.”).

⁴⁰ See Class 1 Comments of Joint Creators and Copyright Owners (*Joint Creators Class 1 Comments*) at 2, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments032715/class%201/Joint_Creators_and_Copyright_Owners_class01_1201

existing exemptions should be renewed. NTIA also supports the notion that pedagogical methods have evolved, both in the classroom and in online education, and that changes in the marketplace necessitate expanding previously-granted exemptions and granting new exemptions for these classes of works.⁴¹ NTIA also offers alternate language in place of “short clips” and “criticism or commentary” in light of proponents’ comments.⁴² Accordingly, NTIA suggests the following exemption for audiovisual works for educational uses:

[2014.pdf](#) (stating that the group “would not oppose a renewal of the educational exemptions for universities and colleges granted in the last proceeding.”).

⁴¹ See *Decherney Petition* at 2 (“High-definition formats have become the prevailing format for audiovisual works distributed today. As technology advances, the means available to faculty and students at education institutions must also advance to incorporate high-definition images and clips into their classroom.”).

⁴² NTIA proposes the language “the length of the clip is no more than is reasonably necessary for such purpose and does not constitute a substantial portion of the original work” in place of “short clips.” Proponents have demonstrated that there is confusion among teachers and students regarding the term “short clips.” See Transcript of May 27, 2015, Hearing on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Section 1201 – Digital Millennium Copyright Act (*May 27 Hearing Transcript*) at 13-14, Docket No. 2014-07, available at <http://copyright.gov/1201/2015/hearing-transcripts/1201-Rulemaking-Public-Roundtable-05-27-2015.pdf> (“[T]he problem is all of this is very vague and subjective.... [W]e’re worried about the short portions language. Someone like Dr. Wallace might say, ‘Well gosh, I think this is short relative to the whole thing.’ But will someone think it is short relative to some other standard? I don’t know what ‘short’ means.”); *id.* at 164-5 (“What I’m suggesting is that the rules about length and brevity contribute to confusion. And a lack of copyright clarity is actually discouraging innovation in the field of digital learning right now.... [T]he law as it was written does not limit fair use to short clips.”). NTIA is also convinced that the record demonstrates that the current language limiting the desired use for the purpose of “criticism or comment” as too narrow and difficult for educators and students to apply. See *Hobbs Class 4 Reply Comments* at 4 (“Teaching and learning is a highly variable practice; situational variation is necessary for education to be responsive to the specific contexts of K-12 education.”). Accordingly, NTIA adopts the modified proposed language of “for purposes of criticism, comment, or education” to include uses permitted under 17 U.S.C. § 107 but also to provide further clarity as requested by proponents. NTIA recommends the additional language here to offer more clarity and to allow proponents to engage in the non-infringing uses identified in their comments while maintaining a tailored exemption.

Motion pictures and similar audiovisual works on DVDs, Blu-Ray discs, or acquired via online distribution services, and protected by various technological protection measures, when circumvention is accomplished solely in order to incorporate excerpts from such works into new works for the purpose of criticism, comment, or education, where the length of the clip is no more than is reasonably necessary for such purpose and does not constitute a substantial portion of the original work,⁴³ and where the person engaging in circumvention believes and has reasonable grounds for believing that circumvention is necessary to fulfill the purpose of the use in the following instances:

- a) Educational use by college and university instructors, faculty, and students;
- b) Educational use by K-12 instructors, and by students in grades 6-12 engaging in video editing projects actively overseen by an instructor;
- c) Educational use by instructors offering Massive Open Online Courses engaged in film and media analysis; and
- d) Educational use by instructors and students participating in digital and media literacy instructional programs in libraries, museums, and non-profit organizations with an educational mission.

Access to Blu-ray Format

NTIA supports including works on Blu-ray discs in the exemptions for audiovisual works for educational uses, a shift from our position in the previous proceeding.⁴⁴ The evidence in this proceeding establishes that the exclusion of high definition material is having an adverse effect on the quality of teaching, and proponents have sufficiently made their case on the record. Proponents argue that students now expect high resolution material, and during the past three years, high definition audiovisual content has become standard across platforms.⁴⁵ Proponents provided many examples of how the prohibition on circumvention has had a negative impact on

⁴³ NTIA uses the term “substantial portion” here to refer only to the quantity of the material used, in comparison to the whole original work. Whether the use is substantial in the qualitative sense is a separate question. *See, e.g., Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 586-87 (1994) (stating that an inquiry into the “amount and substantiality of the portion used” in a fair use determination “calls for thought not only about the quantity of the materials used, but about their quality and importance, too”).

⁴⁴ In that proceeding, NTIA was unconvinced that proponents provided significant evidence of harm or significant evidence that the number of works exclusive to Blu-ray was limited. *See* Letter from Lawrence E. Strickling, Assistant Secretary, NTIA, to Maria Pallante, Register of Copyrights (2012 NTIA Letter), (Sep. 12, 2012), http://www.ntia.doc.gov/files/ntia/publications/ntia_2012_dmca_letter_final.pdf.

⁴⁵ *See Decherney Class I Comments* at 13 (“With the widespread adoption of high-definition televisions and HD-capable media players like Blu-ray players, cable set-top boxes, and streaming boxes, most people experience most audiovisual content in high definition.”); *see also Id.* at 15-16.

criticism and educational uses over the past few years.⁴⁶ Proponents also suggest that failing to grant an exemption could hurt the market for or value of copyrighted works because libraries may not continue to purchase material that professors and students can only use in limited ways.⁴⁷ Opponents offered examples of a range of online management systems that allow users to access high definition copies of films online as alternatives to circumvention.⁴⁸ These options are promising for certain uses. However, proponents demonstrate that these alternatives are not sufficient in most instances.⁴⁹

Opponents assert that screen capture technology has significantly improved in the past three years and is a sufficient alternative to circumvention.⁵⁰ They argue that proponents can use screen capture technology to illustrate “historical events” or other things that do not require subtle image detail.⁵¹ Opponents further suggest that users can also use smartphones or cameras

⁴⁶ See generally *Decherney Class 1 Comments* (stating that students lose interest and divert attention when a clip is presented in a low definition format when they are accustomed to viewing in high-definition, that there is a danger of bias against the material if low definition is used compared to other material in high definition, and that additional information is available in the Blu-ray format that is not present in the lower standard definition); *Hobbs Class 2 Comments* at 5 (“[Teacher Spiro Bolos] showed a video where he conducted some informal classroom research, playing a short clips from Citizen Kane and leading a discussion with two groups of high school students. One group viewed a screencast [screen captured] version of the clip while the other group viewed and discussed a digital clip that had been ‘ripped’. We could clearly see students’ comments were influenced by their ability to see and hear the visual and verbal content of the film.”).

⁴⁷ *Id.* at 22.

⁴⁸ See *Joint Creators Class 1 Comments* at 6 (citing Ultraviolet and Disney Movies Everywhere, cloud-based systems that manage digital content. Further, for an additional \$2-5 charge you can convert a DVD to digital and add it to the Ultraviolet or VUDU account. However, certain studios limit conversion from DVDs).

⁴⁹ See Class 1 Combined Comments at 12, Docket No. 2014-07, available at http://copyright.gov/1201/2015/reply-comments-050115/class%201/EFF_merged_shortform_comments_class01.pdf (comments of Bradley Balach stating, “I work in a school and bandwidth limitations often cause consternation amongst the teachers trying to show video on streaming services in their class rooms. Another issue is that we have a lot of legacy equipment that runs on a VGA (analog) signal. This causes much HDCP enabled content to be unusable with our projectors.”); *id.* at 10 (comments of Benjamin Shell stating, “Online media and DRM have made it very difficult to share media in an offline setting, such as in a presentation at school or work. And some people in America don’t even have access to the Internet (including some close family members and friends). To restrict remixing of freely available materials, or materials which I have a license to access, is to discriminate against certain people, and to limit the ability to communicate in presentations.”).

⁵⁰ See, e.g., *Joint Creators Class 1 Comments* at 9 (“Video capture software has developed significantly over the past three years into an effective tool that allows users to appropriate high quality, broadly compatible images and video from DVD playback which, as the Register stated in the 2012 Report, are suitable for all uses not requiring close analysis.”); Class 1 Comments of AACS LA (*AACS Class 1 Comments*) at 9-11, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%201/AACS_LA_class01_1201_2014.pdf; *May 27 Hearing Transcript* at 63 (Mr. Taylor, representing DVD CCA, noting that, in his opinion, “the video-capture software, or screen-capture software, is a much better alternative to circumvention than it has ever been before.”).

⁵¹ See *AACS Class 1 Comments* at 10-11; *Joint Creators Class 1 Comments* at 5.

to record content.⁵² Unfortunately, in practice these proposed alternatives are often inadequate or unworkable substitutes for access to the originally-purchased copy of the work. It is clear that the quality of clips derived using these methods is insufficient for many necessary uses in educational settings.⁵³ The multimedia evidence submitted on the record by both proponents and opponents, and the demonstrations at the hearings, were helpful for NTIA to assess the current state of these tools.⁵⁴ Information is lost when using screen capture software or physically recording a screen, creating an inferior copy, which negatively impacts the effectiveness of the lesson.⁵⁵ Moreover, some of the same opponents who propose screen capture as an alternative actively seek to thwart screen capture technologies by requiring access control implementers to work to disable such capabilities.⁵⁶ Therefore, while screen capture may be sufficient in some

⁵² See *AACS Class 1 Comments* at 14. NTIA rejects cameras or smartphone recordings as legitimate alternatives to circumvention for the purposes of this exemption.

⁵³ See Class 1 Response to Post-Hearing Questions of Decherney, et al. (*Decherney Class 1 Hearing Response*) at 1, Docket No. 2014-07, available at http://copyright.gov/1201/2015/post-hearing/answers/Class_1_Hearing_Response_Band_Butler_Decherney_Docket_No_2014-07_2015.pdf (“Footage obtained with screen capture technologies is ridden with imperfections, including interlacing, dropped frames, frame rate issues, insufficient resolution, and artifacting”). Further, opponents themselves stated that the difference in quality between a clip obtained through screen capture and from circumvention was discernable to the eye. When asked how someone could tell between a clip obtained through screen capture or a clip created by circumvention, Taylor stated “[u]ltimately, by looking at the – in my opinion, you would look at the actual output and see if it’s less than perfect, then it most certainty probably did not circumvent.”). *May 27 Hearing Transcript* at 59-60.

⁵⁴ See generally Exhibits 13-21, Hearing on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Section 1201 – Digital Millennium Copyright Act, Docket No. 2014-07, available at <http://copyright.gov/1201/2015/hearing-exhibits/> (demonstrating the functionality and limitations of screen capture software that is currently sold on the market).

⁵⁵ Professor Peter Decherney described how the details of the original film are lost when not obtained from the original work, which is possible through circumvention. See *Decherney Class 1 Comments* at 15-18 (“Screen capture also results in a loss of valuable information, including even single frames, which can be essential to rigorous analysis. Just as a book would be incomplete with missing pages, words, and phrases, so would an audiovisual work with missing frames.... High definition video contains information that standard definition does not. The Blu-ray Disc Association explains on its website that Blu-ray discs are designed to convey much more visual information than DVDs: ‘Due to the fact that the data layer on a Blu-ray disc is placed much closer to the laser lens than in DVD, there is less distortion... [h]ence more precision.’”). See also *Decherney Class 3 Comments* at 11 (“[S]tudents in MOOCs experience a transition from the lecturer in HD to the audiovisual excerpt in SD. This disruption in video quality is noticeable and may distract the viewer and dilute the point.”).

⁵⁶ In responding to post-hearing questions from the Copyright Office, DVD CCA and AACS LA acknowledge that “the Robustness Rules for the implementation of the AACS license... require the licensee to protect the content from interception from the point of decryption to the point of display,” making it effectively impossible to perform screen capture when using a licensed Blu-ray player. See Class 1 Response to Post-Hearing Questions of DVD CCA and AACS LA (*DVDCCA Class 1 Response to Post-Hearing Questions*) at 2, Docket No. 2014-07, available at http://copyright.gov/1201/2015/post-hearing/answers/Class_1_Hearing_Response_DVD_CCA_and_AACS_LA_Docket_No_2014-07_2015.pdf (noting that “[a]ttempts to record BD playback will result in a recording of only the audio portion of the content; the video portion appears as a black screen. This result is consistent with the Robustness Rules for the implementation of the AACS license, which require the licensee to protect the content from interception from the point of decryption to the point of display”).

limited circumstances, the Copyright Office should not consider it as a viable alternative to circumvention. When the desired use requires high quality to effectively communicate the message, an exemption should permit educators and students to circumvent the AACCS TPM on Blu-ray discs, in addition to the works available on DVD and through online distribution, and not have to rely on screen capture or recording of the physical display.

Student Use in Grades 6-12

Due to the increasingly sophisticated tools available to students at middle and high school levels, and the need to properly equip students to succeed in the digital world, NTIA supports an expanded exemption to allow students undertaking video editing projects to circumvent TPMs while in grades 6-12.⁵⁷ Proponents have adequately shown adverse effects on noninfringing uses,⁵⁸ and cite a range of examples on the record: (1) TPMs reduce learners' access to film cultural heritage for educational purposes, which diminishes the quality of their education; (2) learners would be placed at an educational disadvantage if forced to rely on movie clip websites; (3) the DMCA is contributing to confusion over legal access to audiovisual clips in education; and (4) restrictions on use of audiovisual works harms the next generation of creators. NTIA recognizes that not all student uses require the quality of clips made possible via circumvention of TPMs. Screen capture technology, despite its limitations, may be sufficient in certain circumstances.⁵⁹ However, screen capture and other alternatives to circumvention are not sufficient to meet all the needs of teachers and students contemplated on the record. When the project or presentation requires a level of quality only available through circumvention, middle and high school students should be permitted to circumvent TPMs when overseen by their instructors. To illustrate, proponents have offered evidence of the necessity of high definition video in student works, such as the National History Fair day (where quality of the video is one of the criteria for judging).⁶⁰

⁵⁷ See Class 2 Renee Hobbs Reply Comments, (*Hobbs Class 2 Reply Comments*) at 2, Docket No. 2014-07, available at http://copyright.gov/1201/2015/reply-comments-050115/class%202/ReplyComments_LongForm_Hobbs_Class02.pdf ("Today, a wide variety of digital tools enable even very young children to create new works by re-purposing existing works in ways that advance their learning. As a novel instructional strategy, research evidence is beginning to demonstrate the effectiveness of digital literacy learning practice. When students use copyrighted materials in creating their own digital works, they demonstrate their understanding of academic content, strengthen collaboration skills, and activate critical and creative thinking. Digital and media literacy learning practices also help children and young people reflect on the social consequence of media in society and take action in the use of information and communication to make a difference in the world.").

⁵⁸ See *Hobbs Class 2 Comments* at 7.

⁵⁹ *Hobbs Class 2 Comments* at 4 (citing a project assigned by Northwest High School where teachers show clips of the film *Chicago* when studying the novel *The Great Gatsby* and the atmosphere of the 1920s. Circumvention of Blu-ray may not be necessary to effectively create these presentations and DVD circumvention or screen capture may suffice).

⁶⁰ See *Hobbs Class 2 Comments* at 3-4; see also How an Entry is Judged? – National History Day, available at <http://pa.nhd.org/judging.htm>. The judging criteria made available online for the National History Day state that judges base 20 percent of a student's overall score on "Clarity of Presentation," which includes consideration of

NTIA is also convinced by the arguments that criticize the current exemption's lack of parity between high school students enrolled in Advanced Placement (*i.e.*, college-level) courses and their university student counterparts.⁶¹ NTIA is sympathetic to concerns that younger students have a less sophisticated understanding of intellectual property laws than older ones, but this alone should not result in the denial of an exemption. Rather, NTIA expects that teachers will properly educate students about copyright infringement and how to utilize works in accordance with statute by developing "best practices" or other guidelines to help clarify any confusion on the part of student. An early conversation about copyright law will aid in deterring infringement by educating young students as to what uses the law permits.

*Massive Open Online Courses (MOOCs)*⁶²

The environment for new learning opportunities is changing rapidly. MOOCs offer a unique learning environment that can be accessed virtually anywhere. Platforms offering MOOCs include Coursera, edX, the Khan Academy, and Udacity.⁶³ Open, often unlimited enrollment online learning should be encouraged, as it allows a breakdown of the traditional barriers to education such as geographic restrictions and limited financial resources.⁶⁴ NTIA supports the development of these innovative tools and opportunities. Yet NTIA also 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.⁶⁵ Therefore, NTIA offers modified language for an exemption covering MOOCs.

whether "the overall project is pleasing to the eye" and "is the visual material clear and appropriate for the type of entry."

⁶¹ See *Hobbs Class 2 Comments* at 6 ("Underscoring the irrationality of the distinctions created by the current set of exemptions is the case of Advanced Placement classes. In 2013, more than 135,000 teachers taught over 2.2 million high school students in AP classes. The objective of the AP program is to enable high school students to take college level classes.... Why should high school students in AP courses have less engaging classroom sessions than students taking similar courses in college?").

⁶² Modifying the language offered by proponents and opponents, NTIA is prepared to define a MOOC for the purposes of this exemption as "a course of study made available over the Internet without charge for the public at large to enroll in." See *Class 3 Comments of Joint Creators and Copyright Owners (Joint Creators Class 3 Comments)* at 13, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%203/Joint_Creators_and_Copyright_Owners_class03_1201_2014.pdf; *May 27 Hearing Transcript* at 105.

⁶³ See *Decherney Class 3 Comments* at 6.

⁶⁴ See *Decherney Class 3 Comments* at 3-4 ("Promulgating exemptions that exclude massive open online courses would arbitrarily disfavor an approach to learning that is an affordable and effective alternative to the traditional classroom. Indeed, studies suggest MOOCs may provide as strong a learning experience as the traditional classroom. In 2010, the Department of Education released a report on online education that concluded, 'classes with online learning (whether taught completely online or blended) on average produce stronger student learning outcomes than do classes with solely face-to-face instruction.'").

⁶⁵ See *Class 4 Comments of the Joint Creators and Copyright Owners (Joint Creators Class 4 Comments)* at 2, Docket No. 2014-07, available at <http://copyright.gov/1201/2015/comments->

NTIA supports granting an exemption for instructors offering MOOCs that require analysis of portions of audiovisual works, when clip length is appropriate for the purpose of criticism, comment, or education, and including TPMs on lawfully acquired DVDs, Blu-ray discs, and online distributed content. NTIA is convinced that the contemplated uses are likely to be noninfringing due to the educational and critical purpose MOOCs serve and the nature of the course medium itself. MOOCs more successfully serve their educational mission if they incorporate visual materials in addition to the video of a lecturing instructor.⁶⁶ As proponents evidenced, MOOCs are generally divided into short video lectures, and the inclusion of audiovisual works must be short in order to accommodate the rest of the lecture.⁶⁷ Based upon the record and the length of lecture videos being created, NTIA believes it is unlikely that instructors would use substantial portions of a work.⁶⁸

NTIA does recognize that, because any Internet user can enroll in a MOOC, there is some concern that a poorly-crafted exemption could further infringement.⁶⁹ Therefore, in seeking to craft an appropriate exemption, NTIA notes 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.⁷⁰ NTIA also supports limiting the exemption to MOOCs that focus on film

[032715/class%204/Joint_Creators_and_Copyright_Owners_class04_1201_2014.pdf](#) (“By the very definition, to the extent there is one, MOOCs are open to anyone, and course enrollment in a single course can in the tens of thousands. In 2014 alone, between 16 and 18 million people participated in a MOOC. Thus, this broad exemption for MOOC students and educators would have broad implication and should be approached with caution.”).

⁶⁶ The record suggests that instructors are finding their lectures to be more effective when they utilize short visual and audio clips to emphasize particular points or principles. *See Decherney Class 3 Comments* at 18 (“[T]he struggle to keep students’ attention is even more relevant in the online classroom. By asking students to navigate to a video content providers such as YouTube, there is the risk that the student will get distracted and not return.”). *See also* Jon Wiener, *Inside the Coursera Hype Machine*, THE NATION, (Sep. 4, 2013) (noting the problems with MOOCs that do not incorporate outside material and stating “[t]here was no attempt to intercut the lecture with visual material, film clips, illustrations, interviews or anything else, and the audio quality was often pretty bad. To young eyes familiar with action movies, fast paced- TV shows and video games, this looks practically Paleolithic.”).

⁶⁷ *See Decherney Class 3 Comments* at 18 (“By design, MOOCs are limited in time. MOOC instructors much teach concepts in video lectures that are typically seven to ten minutes in length, when they would normally have over an hour.”).

⁶⁸ A longer clip of a work might also qualify as a fair use, but a clip that is short in length due to the dictates of a MOOCs video lecture would be more likely to qualify. *See Author’s Guild, Inc. v. HathiTrust*, 755 F.3d 87, 98 (2d Cir. 2014) (noting that the extent of permissible copying varies with the purpose and character of the use); *see also May 27 Hearing Transcript* at 15 (“[I]t’s much more likely to be a fair use if it’s a short clip, right, than a long portion or an entire, say, motion picture. And the record has supported the short clips approach. And it also, I think, at the same time, the language is not so specific that there’s not some room for interpretation”).

⁶⁹ *See Joint Creators Class 3 Comments* at 2.

⁷⁰ *See Decherney Class 3 Comments* at 8-9 (the only examples provided on the record regarding student use are those provided here and do not give a broad enough view into how students may use this exemption). NTIA notes that the other commenters do not mention student uses of this exemption. *See also* Class 3 Comments of the Music Library Association at 1, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_MLA_Class03.pdf. (mentions only primary instructors and support staff and

and media analysis or studies, which would still cover the desired uses noted in proponents' comments.⁷¹ Further expansion of this exemption to all MOOCs is not supported on the record.

The Copyright Office inquired about the TEACH Act (17 U.S.C. § 110) and whether its requirements for formal distance education could be helpful in crafting an exemption.⁷² NTIA does not believe that an exemption based on the TEACH Act would sufficiently address proponents' proposed uses; rather, it would likely cause additional confusion.⁷³ First, the TEACH Act only applies to online course activities that are part of a governmental body or "accredited nonprofit educational institution."⁷⁴ While some MOOC platforms could be classified as the latter, not all MOOCs will qualify.⁷⁵ For example, the National Geographic Society and the Museum of Modern Art are among the Coursera partners that would not fall within these two categories.⁷⁶

music librarians.); Class 3 Comments of the Free Software Foundation at 1, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-020615/FreeSoftwareFoundation/InitialComments_ShortForm_FreeSoftwareFoundation_Class3.pdf (advocates for broadening the proposed exemption to include "any member of an educational institution or organization that uses learning tools or systems such as those used to facilitate MOOCs." They did not advocate for students use). NTIA is not necessarily concerned about the numbers of students that would be able to take advantage of the proposed exemption, but specifically that it is not clear from the record how the students would be able to take advantage of the exemption or how they are currently being harmed. The focus of the evidence in the record is on the instructors using video clips in the design of their MOOC courses. *See, e.g.,* Class 3 Reply Comments of Peter Decherney, et al. at 10-15, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/reply-comments-050115/class%203/ReplyComments_LongForm_DecherneyEtAl_Class03.pdf.

⁷¹ *See Decherney Class 3 Comments* at 8 (citing his desire to offer a MOOC equivalent to his course at the University of Pennsylvania entitled *The Hollywood Film Industry*). While proponents argue that the exemption should cover all MOOCs, NTIA is not convinced that the one cited example of a course outside film or media analysis would require the quality necessary for sophisticated film analysis. *See id.* at 12-13 (Citing the HarvardX course *China*, which "covers the modern society and state that is emerging in China" and "uses audiovisual works to highlight the beauty of the country and provide enrolled students with a sense of its culture.").

⁷² *See Class 3 Post-Hearing Questions from the Copyright Office*, Docket No. 2014-07, *available at* <http://copyright.gov/1201/2015/post-hearing/Letter%20to%20Class%203%20Witnesses-signed.pdf>.

⁷³ Opponents cite the legislative intent behind the TEACH Act to illustrate the point that Congress imposed limitations on Internet-enabled distance learning in order to guard against potential abuse. *See Class 3 Comments of the DVD CCA and AACSLA* at 6, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-032715/class%203/DVDCCA_and_AACSLA_class03_1201_2014.pdf. Proponents argue that lack of litigation that would define the contours of the TEACH Act has resulted in mass confusion for universities that would only multiply if an exemption imposed TEACH Act requirements on MOOCs. *See Class 3 Response to Post-Hearing Questions of Peter Decherney, et al. (Decherney Class 3 Response to Post-Hearing Questions)* at 1, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/post-hearing/answers/Class_3_Hearing_Response_Band_Butler_Decherney_Docket_No_2014-07_2015.pdf.

⁷⁴ 17 U.S.C. § 110 (2012).

⁷⁵ *See Decherney Class 3 Comments* at 16.

⁷⁶ Coursera, *Meet Our Partners*, <https://www.coursera.org/about/partners> (last visited July 20, 2015).

Second, the TEACH Act requirement to place TPMs on the embedded clips should not be included as a condition of an exemption. Currently, the record demonstrates that primary providers of MOOCs do not use TPMs for their online courses.⁷⁷ While the TEACH Act requires TPMs in certain limited circumstances for course content that is digitally transmitted, it is unclear whether this requirement extends to MOOCs, and therefore the Copyright Office should not recommend that an exemption extend this requirement to entities for which the TEACH Act may not apply.⁷⁸ Instead, the decision whether to employ TPMs should be a market decision made by the MOOC providers as to the best method to protect their own works and how best to provide their products to serve their customers.⁷⁹ Further, to the extent the concern here is for possible harm to the original copyright owner (primarily in the re-distribution of their content), the exemption would permit only the clips embedded into lectures, as dictated by the design of MOOCs, that must be short and appropriately tailored for the purpose of the lecture. As such, NTIA is unconvinced that TPMs on MOOC content are necessary to prevent harm to the market for the original work excerpted in a lecture video.⁸⁰ NTIA also notes that no exemption previously granted in this space included this type of restriction. For example, remix videos that rely primarily on short clips obtained via circumvention are disseminated through the Internet via video aggregators such as YouTube, but to date, the Copyright Office has appropriately not required that such videos be protected by access controls. It would only add confusion to suggest that these courses are required to comply with the TEACH Act when that is not necessarily the case.

NTIA does recommend that institutions provide proper notice to instructors and individuals enrolled in MOOCs regarding copyright policies when taking advantage of this exemption, and including such notices in terms of use for the course.⁸¹

⁷⁷ See Class 3 Response to Post-Hearing Questions by DVD CCA and AACSLA (*DVDCCA Class 3 Response to Post-Hearing Questions*) at 2, Docket No. 2014-07, available at: http://copyright.gov/1201/2015/post-hearing/answers/Class_3_Hearing_Response_DVD_CCA_and_AACSLA_Docket_No_2014-07_2015.pdf. The opponents however conclude that any exemption were it to be granted must include the TEACH Act requirements “to protect the movie clip from any unauthorized copying and redistribution.” *Id.* at 5.

⁷⁸ 17 U.S.C. §110(D)(ii)(I) (2012).

⁷⁹ See *Decherney Class 3 Response to Post-Hearing Questions* at 3-5; see also *DVDCCA Class 3 Response to Post-Hearing Questions* at 2 (here the opponents note that “...some magnitude of scale in number of offerings or in the number of distributions, or both, is required to make DRM [digital rights management] scheme economically viable”).

⁸⁰ It should also be noted that most courses or course providers discussed on the record require registration and or payment to gain access to material further eliminating the need to require a TPM as a part of this exemption. This, in effect, limits the audience to the original course content and the capability of just anyone downloading the content and then re-transmitting the content. Further limitations on the ability of the students to download, stream to multiple devices, replay, and copy content should be left to the course instructor and the institution.

⁸¹ See, e.g., 17 U.S.C. 110(2)(D)(i) (2012) (this section provides helpful instruction regarding instituting a copyright policy and promoting copyright compliance - since the TEACH Act does not necessarily apply, this only serves as instruction.).

Museums, Libraries and Non-Profits

Proponents cite multiple examples of museum and library programs that are taking advantage of the rise in digital media in classroom-like settings.⁸² They argue that the lack of an exemption is deterring teaching of digital and media literacy outside of traditional classrooms. They request that “learners” and “educators” in these settings be permitted to circumvent TPMs on audiovisual works.⁸³

Understanding opponents’ contention that the term “nonprofit” is overly broad, NTIA accordingly proposes alternate language for this exemption.⁸⁴ NTIA recommends that an exemption be given to libraries, museums, and non-profits with an educational mission that offer instructional courses. NTIA recommends this exemption in addition to the one proposed in Class 6, discussed in the next section. While the desired uses may overlap, at times, with the uses in noncommercial remix videos contemplated in Class 6, the desired uses for museum, libraries, and non-profits have a strictly educational purpose.⁸⁵ The proponents advocate to include both educators and learners in this exemption, which NTIA supports.⁸⁶

⁸² See Renee Hobbs Class 4 Comments (*Hobbs Class 4 Comments*) at 2, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_HobbsEtAl_Class04.pdf (“Over the past seven years, the John D. and Catherine MacArthur Foundation has invested more than \$150 million in understanding new forms of learning in informal, interest-driven networks that use the powerful new creative and expressive tools of digital media. To understand how learning is changing as a result of the rise of digital media, they developed a research hub at the University of California, Irvine and established other innovative programs such as the YouMedia program at the Washington Public Library in Chicago.”) *Id.* at 4 (“The LAMP NYC [is] New York City non-profit organization that offers media literacy programs as afterschool and summer programs. The LAMP has created MediaBreaker, which is an online remix tool that enables learned [sic] to critically analyze media through a commenting tool that slows down the viewing experience and activates a set of critical question designed to strengthen media analysis skills.”) (“[T]he Media Spot is a Brooklyn-based non-profit organization that works to provide elementary and secondary school teachers with professional development experiences to support their growth as digital learners.”).

⁸³ See *Hobbs Class 4 Comments* at 2-5.

⁸⁴ See Class 4 Comments of Joint Creators at 4, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments032715/class%204/Joint_Creators_and_Copyright_Owners_class04_1201_2014.pdf.

⁸⁵ For example, proponents cite the work of Jeannine Cook, the lead educator for the media and Technology Program at YESPHILLY, a non-profit organization that helps out-of-school African American youth get their GED. A project that she assigns is a “poetry video” where students wish to incorporate clips of culturally-relevant films. This might be characterized as a noncommercial, remix video, where circumvention is permitted under Class 7. However, proponents also cite to other examples of uses that are strictly centered on education such as the *See Renee Hobbs Class 4 Reply Comments* at 5, available at http://copyright.gov/1201/2015/reply-comments-050115/class%204/ReplyComments_LongForm_Hobbs_Class04.pdf; see also *May 27 Hearing Transcript* at 233 (“[I] don’t think that, although it’s possible, as we discussed before, that [the exemption for remix videos] might apply, I don’t think it makes much sense to consider the work that happens in libraries, museums, and nonprofit organizations around digital learning to be painted with the same brush as the work of remix video artists.”).

⁸⁶ See, e.g., *Hobbs Class 4 Comments* at 2.

2. Filmmaking and Other Derivative Work Creation (Classes 5-7)

Three proposals seek to renew and expand current exemptions for filmmaking and other derivative uses to include fictional works and works on Blu-ray. The proposed classes cover multimedia e-books,⁸⁷ noncommercial remix videos, and derivative filmmaking uses.⁸⁸ Previous exemptions have allowed filmmakers, authors, and remix artists to make fair use of protected works.⁸⁹ However, industry expectations that works be produced in high definition show the limits of the current exemption. NTIA supports renewal of these existing classes and expansion to include works distributed on Blu-ray discs. NTIA also suggests changes to language from the previous exemptions.⁹⁰ The record for Blu-ray is more substantial in this proceeding than it has been in the past, and as high definition formats become the norm for the filmmaking and remix industries, its inclusion in the exemption is justified and supported by the record. Accordingly, NTIA suggests the following exemption:

⁸⁷ The record did not support expanding this exemption to cover all types of multimedia e-books. From the record, it is unclear whether or not the proponents took advantage of the exemption granted previously. Therefore, NTIA recommends only renewing the previous exemption and expanding it to include Blu-ray. This exemption is designed to include works such as Professor Samuelson's Copyright Law e-book as it requires close analysis of film clips from James Bond movies to evaluate character qualities, even though it is a legal textbook.

⁸⁸ See Class 5 Comments of Author's Alliance, et al. (*Author's Alliance Class 5 Comments*), Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_AuthorsAllianceEtAl_Class05.pdf; see also IDA Class 6 Comments; Class 7 Comments of the Electronic Frontier Foundation and Organization for Transformative Works (*EFF Class 7 Comments*), Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_EFFOTW_Class07.pdf.

⁸⁹ See Class 6 Comments of New Media Rights (*NMR Class 6 Comments*) at 15, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_NewMediaRights_Class06.pdf (Nothing that filmmaker Michael Singh could not have created the film *Valentino's Ghost*, a documentary that looked at Hollywood's bigotry and Islamophobia using clips obtained through circumvention of CSS systems on DVDs, without the exemption because "while the film obviously constituted fair use, [Singh] would have been barred from accessing vital motion picture clips due to Section 1201(a)(1)."). See *EFF Class 7 Comments* at 3 (citing that roughly 6.5 million people have produced remix videos in the United States and offering many examples of remixed videos created in the past 3 years).

⁹⁰ Proponents for Class 7 requested broader language "for the purposes of fair use." See Initial Petition of the International Documentary Association, et al., Docket No. 2014-07, available at http://copyright.gov/1201/2014/petitions/International_Documentary_Association_et_al_1201_Initial_Submission_2014.pdf. NTIA offers language that aims to include most fair uses identified by proponents in their request, but that also provides the necessary guidance for users of the exemption. See *IDA Class 6 Comments* at 19-20 ("A quantitative limit would not provide additional guidance for those who wish to utilize the exemption, but could instead create unintended consequences by undermining the principle that when making fair use, filmmakers must use only what they need and no more.").

Motion pictures and similar audiovisual works on DVDs or Blu-Ray discs, or acquired via online distribution services, and protected by various technological protection measures, when circumvention is accomplished solely in order to incorporate excerpts from such works into new works for the purpose of criticism, comment, or education, where the length of the clip is no more than is reasonably necessary for such purpose and does not constitute a substantial portion of the original work, and where the person engaging in circumvention believes and has reasonable grounds for believing that circumvention is necessary to fulfill the purposes of creating:

- a) Nonfictional or educational multimedia e-books offering film analysis;
- b) Noncommercial videos;⁹¹
- c) Documentary films; and
- d) Narrative films portraying real events, where the prior work is used for its biographically or historically significant nature.

Access to Blu-ray Format

Proponents have met their burden of proof and provided substantial evidence of negative impacts on criticism, justifying a renewal of previous exemptions with an expansion to include Blu-ray.⁹² The proponents showed that the quality of clips obtained from DVDs is substantially less than that of Blu-ray.⁹³ They cite film and television distribution standards that require use of high definition video.⁹⁴ Opponents proposed alternatives to circumvention of Blu-ray discs such

⁹¹ In 2012, NTIA supported a definition of “primarily noncommercial works” to reiterate that some commercial uses are also fair use. *2012 NTIA Letter* at 24. As in the previous proceeding, the record shows that many videos in this class are made by interest groups and nontraditional organizations that lack in-house expertise to make these videos and they will contract out video projects. For example the NCAI hired an outside firm to make “Take it Off” regarding the Washington Redskins trademark. *EFF Class 7 Comments* at 23-24. Proponents argue that a lack of resources should not bar a finding of fair use. *Id.* at 24. However, since the Copyright Office in the previous proceeding was explicit in including such uses within their exemption, NTIA supports renewing the exemption for noncommercial remix videos, with the carve out for commissioned uses. *See 2012 Final Rule* at 65,266 (“For purposes of this exemption, ‘noncommercial videos’ includes videos created pursuant to a paid commission, provided that the commissioning entity’s use is noncommercial.”).

⁹² *See, e.g., IDA Class 6 Comments; EFF Class 7 Comments; Comment of New Media Rights (New Media Class 7 Comments)*, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_NewMediaRights_Class07.pdf.

⁹³ *See EFF Class 7 Comments* at 29 (Stating there are 345,600 pixels per video frame for the DVD format, compared to the 2,073,600 pixels per video frame for Blu-ray).

⁹⁴ *See, e.g., IDA Class 1 Comments; May 27 Hearing Transcript* at 9-10 (“Standard definition DVD quality images are being rejected on our programs by our distributors ranging from Magnolia Films to CNN. And there is a change in the way theaters show films. They don’t show film anymore. They show digital cinema packs and they have to be

as up-conversion, licensing, and screen capture software.⁹⁵ NTIA does not find these alternatives adequate for the uses contemplated in this proposed class. Filmmakers note significant difficulties in using up-conversion to derive clips of sufficient quality.⁹⁶ Further, the ability to license clips is not a sufficient alternative due to difficulties in negotiation for clips that the copyright owners may have an incentive to withhold.⁹⁷ Further, courts have held that lost licensing revenue does not automatically favor the copyright owner in a fair use analysis with regard to the fourth statutory factor (“effect of the use upon the potential market for or the value of the copyrighted work”).⁹⁸ Screen capture—as discussed in the previous section on educational uses, and when it is even technically possible—creates a product that is inferior in quality to the product accessed via circumvention.⁹⁹ It is not an alternative for filmmakers whose art dictates

created in a minimum of HD quality.” Proponents also note they had to undergo significant changes to the award-winning documentary “Life Itself” before distributors accepted it for play.). *IDA Class 6 Comments* at 69 (Statement of Joseph Stillman stating that PBS would not accept his documentary *From Mills River to Babylon and Back . . . The Jimmy Massey Story* because it was in SD).

⁹⁵ See Class 6 Comments of AACLS LA (*AACLS Class 6 Comments*) at 8-10, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%206/AACLS_LA_class06_1201_2014.pdf

⁹⁶ See *IDA Class 6 Comments* at 27 (“Required up-conversion of DVD content from 720 pixels (horizontally) to 4840 pixels (horizontally) is a difficult and costly process, and unacceptable visually on a 4K UHH TV, much less a 60 foot wide theater screen.”); *id.* at 27-28 (“The process of creating a [Digital Cinema Pac] for theatrical screening requires additional conversion of EVERY frame of the video into individual still frames (1,440 per minute). During this process the ‘fake’ frames behave differently than the actual frames from the DVD and create another level of image degradation beyond just the up-conversion to HD. DCP files also require conversion of the video from RGB color space to XYZ color space to adhere to the strict DCP specification. Interpolated video frames from DVD up-conversion to HD get degraded into the conversion to XYZ color space as well.”); *May 20 Hearing Transcript* at 101-102 (“In order to do up-conversion, you either have to have Jim Morrisette, who is a trained engineer who has been doing this for 40 years, who works equipment that can’t be rented out because it’s so complex, or you have to send it out to a processing house and that can cost several hundred dollars an hour to work with a short clip.”).

⁹⁷ See, e.g., *IDA Class 6 Comments* at 13 (“[T]he documentary *Inequality for All* relied on the fair use exemption for documentary films to show an interview with the president of Viacom, Inc. that painted the president in a bad light. The filmmakers attempted to license the clip, but were given a no-explanation turndown letter. Without fair use and the proposed exemption, they would have been unable to use the footage.”); *id.* ([C]learance specialist Kenn Rabin attempted to license a clip he had previously licensed for a previous project- a clip depicting an American soldier during the Vietnam War smoking marijuana out of his rifle. He was denied use of the clip for the second project, and the reason he was given was that the rights holder did not want to license any negative depictions of American troops while we were at war. Unfortunately, the DVD clip of the footage was of insufficient quality for the project, and so the filmmakers abandoned the use of the clip entirely.”).

⁹⁸ 17 U.S.C. § 107(4) (2012); See *Bill Graham Archives v. Dorling Kindersley, Ltd.*, 448 F.3d 605, 614 (2d Cir. 2006) (“[W]ere a court automatically to conclude in every case that potential licensing revenues were impermissibly impaired simply because the secondary user did not pay a fee for the right to engage in the use, the fourth factor would *always* favor the copyright holder.... Instead, we look at the impact on potential licensing revenues for ‘traditional, reasonable, or likely to be developed markets.’”).

⁹⁹ See *IDA Class 6 Comments* at 14 (“[Screen capture] presents a real question of legality to filmmakers who are concerned about violating the DMCA because it is not clear whether the copyrighted material is captured before or after decryption. It still have unacceptable stuttering, dropped frames, and image size issues. Finally, there is no screen capture software available for Blu-ray on the Mac platform used by a majority of filmmakers.”).

quality of presentation.¹⁰⁰ The uncertainty over the extent to which some platforms prohibit screen capture software from working (likely due in part to license agreements between rights holders and vendors, such as the AACCS license agreement) is also concerning.¹⁰¹ Proponents further note the difficulty in using material that is only available on Blu-ray disc.¹⁰²

Proponents for the remix video exemption also provided compelling material supporting their request. They cited audiovisual works that were necessary for use in their remix videos, offering as an example commentary that is only available on Blu-ray (such as special features and audio commentary).¹⁰³ Proponents also provided an informative demonstration of the sophisticated video editing required to create their videos, and explained that high initial quality is necessary to carry out those edits and end up with an acceptable final product.¹⁰⁴ NTIA recommends renewing the exemption from the previous rulemaking and expanding it to include the Blu-ray format.

Filmmaking Uses

Proponents have created a record that supports an expansion of the previous exemption for documentary filmmakers.¹⁰⁵ Proponents requested an exemption for all filmmakers, including those creating both documentary and narrative films, for the purposes of fair use.¹⁰⁶ They argue

¹⁰⁰ See *IDA Class 6 Comments* at 27-29 (noting that documentary distribution has expanded since 2012 into film festivals and theatrical release, where over 90 percent of all movie theaters in the U.S. now have digital projectors that use Digital Cinema Pac formatted files that must be at least 1920x1080 pixels—a standard definition DVD is 720x480 pixels).

¹⁰¹ See *DVDCCA Class 1 Response to Post-Hearing Questions* at 2; *May 27 Hearing Transcript* at 243-245.

¹⁰² See *IDA Class 7 Comments* at 30-32.

¹⁰³ See *EFF Class 7 Comments* at 12 (One remix artist noting the importance of special extras exclusive to Blu-ray such as behind the scenes footage and deleted scenes. They state these materials are critical for creating remixes because they expand the artist's options and are particularly important for vides based on movie sources where footage is limited and the "extras or deleted scenes might be necessary to round out the story I'm trying to tell.").

¹⁰⁴ See *EFF Class 7 Comments* at 17 ("[Screen capture] software is not designed to output footage that can be used in nonlinear editing programs – the programs needed to create remixes. Each type of editing – applying effects, filters, time changes, or even simply editing different clips together in a montage and then producing a final output file – necessarily degrades quality further.").

¹⁰⁵ NTIA accepts the definition widely used by courts and supported by proponents. A documentary film is a film that "comprises interviews with real people and depictions of real events that are intended to provide a factual record or report." See *Class 6 Response to Post-Hearing Questions of Michael C. Donaldson, et al. (Donaldson Class 6 Hearing Response)* at 1, Docket No. 2014-07, available at http://copyright.gov/1201/2015/post-hearing/answers/Class_6_Hearing_Response_Lerner_et_al_Docket_No_2014-07_2015.pdf (quoting *Psenicksa v. Twentieth Century Fox Film Corp.*, 409 F. App'x 368, 370 (2d Cir. 2009)).

¹⁰⁶ See *Initial Petition of the International Documentary Association, et al.*, Docket No. 2014-07, available at http://copyright.gov/1201/2014/petitions/International_Documentary_Association_et_al_1201_Initial_Submission_2014.pdf.

that fair use decisions are focused on the “specific use in question, not general characteristics of the genre,” noting that “[b]oth documentary and narrative films entertain as well as educate, and inspire, as well as inform.”¹⁰⁷ NTIA agrees that an exemption is warranted for genres of film beyond documentaries, but is uncertain that the record supports including all narrative filmmaking at this time. In particular, it is not clear how expansive the term “narrative” filmmaking is.¹⁰⁸ However, proponents have identified many proposed film projects where the use of prior audiovisual works would likely be fair use, but do not strictly fall within the category of documentary filmmaking. In particular, the comments suggesting such films as “biopics” be included in an exemption were helpful in further refining our proposed language.¹⁰⁹ As the Section 1201 exemptions are intended to provide clear guidance, NTIA supports a modified exemption for a limited number of non-documentary film genres that are closely aligned with courts’ findings of fair use and the proponents’ desired uses.¹¹⁰

The exemption aims to include filmmaking of biopics and other similar films using clips from other works to engage in criticism, commentary, or education. NTIA also supports the use of motion pictures and similar audiovisual works in other fictional films when the nature of the clip used in the film is necessary to comment on the historically-based plot of the film, or when necessary to show its biographical significance. NTIA is convinced that such uses are likely fair use and that the exemption proposed closely aligns with precedent. For example, in a recent case, a musical depicting the dramatized history of the band The Four Seasons used a portion of an episode of *The Ed Sullivan Show* that depicted the television host introducing the band, indicating an important moment in the band’s celebrated career.¹¹¹ The Ninth Circuit held that

¹⁰⁷ See *IDA Class 6 Comments* at 7.

¹⁰⁸ See Class 6 Comments of Joint Creators and Copyright Owners (*Joint Creators Class 6 Comments*), Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%206/Joint_Creators_and_Copyright_Owners_class06_1201_2014.pdf; *May 20 Hearing Transcript* at 30-33.

¹⁰⁹ See *Donaldson Class 6 Hearing Response* at 3. Proponents argue that terms such as “biopic” and “based on a true story” lack any commonly accepted meaning and are frequently used as marketing ploys. NTIA suggests language to include filmmaking portraying real events, while requiring that use of prior clips have biographical or historical significance to the story of the new work and focusing on the transformative nature of resultant works. Despite proponent’s claim, NTIA is not convinced an exemption for “films that portray real events” offers any further guidance than narrative films.

¹¹⁰ Proponents advocate that all fair use purposes be included in the exemption. See *IDA Class 6 Comments* at 2. NTIA proposes modified language regarding the purpose of the use in order to provide clear guidance for those who wish to make use of the exemption. In determining whether use of copyrighted work is fair, courts generally consider the purpose and character of use, the nature of the copyrighted work, the amount and substantiality of the portion used in relation to the work as whole, and the effect of the use on the potential market for or value of the work. See, e.g., *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, (1994); *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 551 (1985). For a searchable centralized list discussing fair use cases, please see the “Fair Use Index” created by the Copyright Office available at <http://copyright.gov/fair-use/>.

¹¹¹ A seven-second excerpt from the Ed Sullivan show that showed the TV host introducing the band’s performance on the TV show used in the Broadway musical production of *Jersey Boys*, a fictionalized account of the Four Seasons, was fair use. *Sofa Entm’t, Inc. v. Dodger Productions, Inc.*, 709 F.3d 1273, 1278 (9th Cir. 2013) (“Dodger references the Four Seasons’ performance on the January 2, 1966 episode of *The Ed Sullivan Show* to mark an

“by using the clip for its biographic significance, [the defendant] has imbued it with new meaning and did so without usurping whatever demand there is for the original clip.”¹¹² While this was a musical production, and it is not clear whether circumvention was required, the example is offered to illustrate the types of storytelling NTIA would support in the exemption. As courts have found repeatedly, fair use provides fictional artists with the same privileges that nonfictional artists enjoy, provided that they meet fair use standards.¹¹³ Fair use distinguishes uses like these from other filmmaking settings where the work is not transformative and obtaining a license is more appropriate.¹¹⁴ Application of the anti-circumvention provisions should encourage artists to invest in their own productions, while encouraging commentary and criticism of prior works in accordance with fair use. The modest expansion in this case to include biopics and other fictional films depicting historical events is warranted by the record and supports this policy goal.

important moment in the band’s career. At that point in rock & roll history, many American bands were pushed into obscurity by the weight of the ‘British Invasion....’ Being selected by Ed Sullivan to perform on the show was evidence of the band’s enduring prominence in American music. By using it as a biographical anchor, Dodger put the clip to its own transformative ends.”).

¹¹² 709 F.3d at 1276.

¹¹³ See, e.g., *Arrow Productions v. The Weinstein Company*, No. 13-Civ.-5488 (S.D.N.Y. 2014); *Bourne Co. v. Twentieth Century Fox Film Corp.*, 602 F. Supp. 2d 499, 511 (S.D.N.Y. 2009); *Faulkner Literary Rights, LLC v. Sony Picture Classics, Inc.*, 953 F. Supp. 2d 701 (N.D. Miss. 2013).

¹¹⁴ While use of the term “transformative” can be helpful, the courts are not necessarily in agreement on how that term applies with respect to the fair use analysis. See, e.g., *Kienitz v. Sconnie Nation LLC*, 766 F.3d 756, 758-59 (7th Cir. 2014) *cert. denied*, 135 S. Ct. 1555. Transformative use of a work is generally considered to be fair use when the new work does not supersede the original creation, but “instead adds something new, with a further purpose of different character, altering the first with new expression, meaning, or message.” See *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569 (1994). For a different view of how to apply this analysis, see *Cariou v. Prince*, 714 F.3d 694, 707-08 (2d Cir. 2013) (finding a transformative use when looking at the work, the court concluded: “the photographs... have a different character, give [the original] photographs a new expression, and employ new aesthetics with creative and communicative results distinct from [the originals].... [However,] merely presenting the same material in a new form... is not transformative.” Here the new works did not present the same material but instead “‘added something new’ and presented images with a fundamentally different aesthetic.”(citations omitted)).

3. Space Shifting and Format Shifting (Class 8)¹¹⁵

Proponents have requested an exemption that would allow circumvention of TPMs on “motion pictures and other audiovisual works on lawfully made and lawfully acquired DVDs, Blu-ray discs... and downloaded files, when circumvention is accomplished for the purpose of noncommercial space shifting of the contained audiovisual content.”¹¹⁶ “Space shifting,” also known in some contexts as “format shifting,” is the act of producing “a copy of a work for the express purpose of non-commercially and personally perceiving it on a device other than the one for which it was originally intended.”¹¹⁷ Similar to the previous rulemaking, Public Knowledge is requesting a space shifting exemption because, due to the evolving technological landscape, “the ability for [consumers] to continue to access and enjoy [purchased copies of audiovisual works] into the future depends in significant part upon their ability to shift the works between devices and formats.”¹¹⁸ Other proponents cast the issue in a slightly different light; the Music Library Association, for example, notes that “space- and format-shifting are important preservation practices that ensure continued access to important musical materials as format and playback technology become obsolete.”¹¹⁹

NTIA acknowledges that there has been considerable debate over whether, and under what circumstances, space shifting may be considered a noninfringing use. During the previous triennial rulemaking, NTIA supported an exemption for space shifting in the interest of consumer protection. NTIA then noted that “many consumers have accumulated large collections of DVDs that lack alternatives introduced since the format was first introduced, and absent the ability to space shift, they may lose access to those motion pictures as the market continues to shift towards mobile and Internet-dependent devices.”¹²⁰ Further, NTIA found that proponents in that

¹¹⁵ NTIA notes that the Copyright Office appears to have grouped the space shifting petition with a separate, unrelated petition. *See 2014 NPRM* at 73,862 (“in the context of a general objection to digital rights management technology, Alpheus Madsen has requested an exemption to allow circumvention of CSS for purposes of playing DVDs on the Linux Operating System”). That request appears to be distinct from space shifting or format shifting because the proponent did not contemplate creating a new, non-ephemeral copy of the work, but merely sought to decrypt a legally-purchased DVD for playback on Linux, an operating system he alleges lacks licensed players. *See Initial Petition of Alpheus Madsen*, Docket No. 2014-07, *available at* http://copyright.gov/1201/2014/petitions/Madsen_Alpheus_1201_Initial_Submission_2014.pdf. NTIA takes no position on this petition because the record for this particular proposal was not further developed after it was subsumed under space shifting.

¹¹⁶ *See Initial Petition of Public Knowledge* at 1, Docket No. 2014-07, *available at* http://copyright.gov/1201/2014/petitions/Public_Knowledge_1201_Initial_Submission_2014.pdf.

¹¹⁷ *2012 NTIA Letter* at 31.

¹¹⁸ *See Class 8 Comments of Public Knowledge (Public Knowledge Class 8 Comments)* at 14, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_PublicKnowledge_Class08.pdf.

¹¹⁹ *Class 8 Comments of the Music Library Association* at 1, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_MLA_Class08.pdf.

¹²⁰ *2012 NTIA Letter* at 33.

proceeding were persuasive in arguing that space shifting is fair use, particularly where DVDs “are not accompanied by an additional copy in any other format, online, or through alternative solutions such as Ultraviolet and Managed Copy.”¹²¹ However, “while the Register was sympathetic to the desire to consume content on a variety of different devices,” the Register disagreed in the 2012 rulemaking that space shifting would be noninfringing under current law.¹²²

NTIA emphasizes our respect for the Copyright Office’s considerable expertise in the field of copyright law, and appreciates that the result in this proceeding may be the same as in the last proceeding. The disagreement between our two offices is reflective of a larger debate over the merits and legality of noncommercial space shifting. That said, NTIA’s view that space shifting is likely noninfringing is grounded in credible legal theory advanced by experts in the field as well as in case law. In an article exploring the legacy of *Sony v. Universal*, copyright scholar Pamela Samuelson notes that “format shifting, that is, transforming a digital file from, for example, a WMA to an MP3 format in order to be able to listen to the file on an MP3 player, is a common and well-accepted practice.” Further, she is persuaded that “platform shifting, that is, making a copy of a digital work to make it playable on a different device is similarly widely accepted as fair.”¹²³ Equally noteworthy, proponents cite a number of congressional documents and legal proceedings in making their case on the record. Public Knowledge cites a House Report and House hearings on the 1971 Sound Recording Act as evidence of the longstanding understanding that personal, noncommercial copying of legally-obtained works is fair use, and points to a 1961 report by the Copyright Office to the same effect.¹²⁴ Proponents further note that, “in the intervening years since [*Sony v. Universal*], no court has found personal, noncommercial space-shifting of the sort proposed here to be an infringement of copyright.”¹²⁵ To the contrary, related cases have been few and far between,¹²⁶ and while no case has dealt

¹²¹ *Id.* at 32.

¹²² 2012 *Final Rule*, 77 Fed. Reg. 65,260, 65,277.

¹²³ Pamela Samuelson, *The generativity of Sony v. Universal: The Intellectual Property Legacy of Justice Stevens*, 74 *FORDHAM L. REV.* 1831, 1866 (2006).

¹²⁴ *Public Knowledge Class 8 Comments* at 3-4.

¹²⁵ *Id.* at 5.

¹²⁶ In the hearing on space shifting, the Copyright Office asked whether there was any case law on making noncommercial, personal-use copies of (non-digital) books. None of the witnesses were aware of any such case despite the fact that physical books have been distributed for as long as U.S. copyright law has existed. Proponent Sherwin Siy, from Public Knowledge, said he found it interesting “that we don’t see any case law indicating that would be an infringement.” Transcript of May 19, 2015, Hearing on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Section 1201 – Digital Millennium Copyright Act (*May 19 Hearing Transcript*) at 150, Docket No. 2014-07, available at <http://copyright.gov/1201/2015/hearing-transcripts/1201-Rulemaking-Public-Roundtable-05-19-2015.pdf>.

specifically with the activity contemplated by proponents, the courts generally seem to point towards space shifting as being a fair use.¹²⁷

Opponents in this proceeding reject the idea that space shifting is fair use, stating that, “as the Register and the Librarian have concluded in the past, the statutory factors for analyzing fair use claims weigh against a determination that format-shifting and space-shifting are fair uses.”¹²⁸ Moreover, the Joint Creators claim that “not one of the four factors weighs in favor of a conclusion that space-shifting and format-shifting are fair uses,” asserting that the nature of the use is not transformative, that creative works are by nature negative indicators of fair use rights, that space shifting “involves reproducing entire works of authorship,” and that “emerging online services would be harmed” by the proposed use.¹²⁹ However, opponents do not explain why space shifting and format shifting should be considered legally distinct from time shifting, an activity explicitly deemed to be fair use by the Supreme Court in *Sony v. Universal*. Both the purpose and the technical details of time and space shifting are similar; in both instances, the user lawfully obtains an audiovisual work and changes the medium or format in which it is contained to enable future viewing.

Debates about the permissibility of space shifting aside, parties have contributed a wealth of evidence about harms endured due to the prohibition against circumvention, as well as alleged alternatives to circumvention that may mitigate those harms. Opponents point to the rise of streaming media services, and in particular multi-platform systems like UltraViolet—which, according to the DVD Copy Control Association (DVD CCA) and the AACS Licensing Administrator (AACS LA), “currently has over 19 million US subscribers” and “a library of over 10,000 titles.”¹³⁰ Importantly, they note that “for many Blu-ray discs, the content companies provide UltraViolet rights for that title included in the price.”¹³¹ NTIA appreciates the potential

¹²⁷ To illustrate, Public Knowledge cites to *RIAA v. Diamond Multimedia Systems* where the court held that “‘merely mak[ing] copies in order to render portable, or space-shift’ media is a ‘paradigmatic noncommercial personal use’”. Public Knowledge concludes that such reasoning is based on an “express analogy to the Supreme Court’s holding in *Sony* with respect to time-shifting.” See Class 8 Reply Comments of Public Knowledge (*PK Class 8 Reply Comments*) at 4, Docket No. 2014-07, available at http://copyright.gov/1201/2015/reply-comments-050115/class%208/ReplyComments_LongForm_PublicKnowledge_Class08.pdf (quoting *RIAA v. Diamond Multimedia Systems*, 180 F. 3d 1072 (9th Cir. 1999)). Public Knowledge also argues that the case *Fox Broadcasting Co. Inc., v. DISH Network, LCC* provides additional insight in this area, though this case is still being litigated. *Id.* at 3 (citing and referencing to *Fox Broad. Co. Inc. v. Dish Network, L.C.C.*, 905 F. Supp. 2d 1088, (C.D. Cal. 2012) *aff’d sub nom. Fox Broad. Co. v. Dish Network L.L.C.*, 723 F.3d 1067 (9th Cir. 2013) (en banc) and *aff’d sub nom. Fox Broad. Co. v. Dish Network L.L.C.*, 747 F.3d 1060 (9th Cir. 2014)).

¹²⁸ Class 8 Comments of Joint Creators and Copyright Owners (*Joint Creators Class 8 Comments*) at 2, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%208/Joint_Creators_and_Copyright_Owners_class08_1201_2014.pdf.

¹²⁹ *Id.* at 3-4.

¹³⁰ Class 8 Comments of DVD CCA and AACS LA (*DVD/AACS Class 8 Comments*) at 9, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%208/DVDCCA_and_AACS_LA_class08_1201_2014.pdf.

¹³¹ *Id.*

for such an arrangement, which enables consumers to lawfully experience works on a range of devices and formats. We note, however, that such services have not been made available with the large majority of the physical media ever sold. UltraViolet and similar services have only existed for a few years, and despite growing libraries, they do not rival the body of works available via DVD or Blu-ray.¹³²

Much of the evidence of harm on the record highlights the real-world difficulties users encounter when attempting to play back copies of motion pictures they previously purchased. John Cleave notes that “DVDs are relatively fragile,” and that he personally has “had at least a dozen movies [he] legally purchased become unusable due to defect or machine incompatibility”—a problem that might have been prevented had he been “allowed to make a backup to cover such an event.”¹³³ Another proponent makes a similar point, commenting that he has “kids, kids that don’t understand that these shiny disks[sic] aren’t just toys.”¹³⁴ Other commenters focus on the considerable investments they have made in their motion picture libraries. Art Miller reports that, if he were “to re-buy all of [his] music, audio books, books, movies and tv shows [he’d] spend several thousand dollars.”¹³⁵ Dan Falconer also says “it would cost [him] thousands of dollars to get digital copies of [his] DVD’s, many of which are not available” on Internet-based services, and he further notes that “the available digital formats require access to an external service, which means [he’ll] lose them if that service goes away.”¹³⁶ NTIA is persuaded that many Americans have made considerable investments in copies of motion pictures distributed on physical media; the possibility that they might spend hundreds or even thousands of dollars on new copies in the latest formats should not be seen as a viable alternative to circumvention. Moreover, consumers can only take advantage of Internet-based distribution services like UltraViolet if they have the means and ability to use high-speed Internet services. NTIA shares Public Knowledge’s fear that denial of this exemption could “add another disadvantage to populations that are already being left behind by technological advancement,” due to the unavailability or expense of adequate broadband connections.¹³⁷

Similar to the previous proceeding, NTIA is again persuaded that the record supports a narrowed version of the proposed exemption. Specifically, the evidence on the record is overwhelmingly focused on the harm to consumers due to their inability to space shift motion pictures on physical media, namely DVDs and Blu-ray discs. The record does suggest this harm

¹³² For example, in the hearing on space shifting, Public Knowledge representative Sherwin Siy noted the difficulty of obtaining the true number of titles available on DVD, but noted that their “initial check on this just in terms of what is available on Amazon in hard copy format comes to 810,000.” *May 19 Hearing Transcript* at 153.

¹³³ See Class 8 Combined Comments at 1, Docket No. 2014-07, available at http://copyright.gov/1201/2015/reply-comments-050115/class%208/EFF_merged_shortform_comments_class08.pdf.

¹³⁴ *Id.* at 2.

¹³⁵ *Id.* at 8.

¹³⁶ *Id.* at 21.

¹³⁷ *Public Knowledge Class 8 Comments* 15-16.

is significantly mitigated where access to the work in digitally-delivered format is bundled with the physical copy. As a result, NTIA recommends an exemption similar to the one we recommended in 2012,¹³⁸ edited to reflect the increased record on motion pictures distributed on Blu-ray discs:

Motion pictures on lawfully acquired DVDs or Blu-ray discs, when the disc neither contains nor is accompanied by an additional copy of the work in an alternative digital format, and when circumvention is undertaken solely in order to accomplish the noncommercial space shifting of the contained motion picture.

B. Literary Works Generally

1. Interoperability with Assistive Technologies (Class 9)

The American Foundation for the Blind, American Council of the Blind, and the Library Copyright Alliance seek renewal of the current exemption, which allows 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 electronically distributed literary works (“e-books”).¹³⁹ The Librarian has granted an exemption for this particular purpose since 2003.¹⁴⁰

NTIA supports renewing this exemption because 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.¹⁴¹ Most e-books continue to be sold or distributed with some form of TPM, which in many cases renders the content completely inaccessible to the visually impaired and print disabled.¹⁴² Many Americans are thus adversely affected when they cannot use assistive

¹³⁸ In 2012, NTIA proposed the following exemption: “Motion pictures on lawfully acquired DVDs that are protected by the Content Scrambling System, when the DVD neither contains nor is accompanied by an additional copy of the work in an alternative digital format, and when circumvention is undertaken solely in order to accomplish the noncommercial space shifting of the contained motion picture.” *2012 NTIA Letter* at 32.

¹³⁹ Class 9 Comments of American Foundation for the Blind et al. (*AFB Class 9 Comments*) at 2, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_AFBetal_Class09.pdf.

¹⁴⁰ See Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. RM 2002-4E, *Final Rule*, 68 Fed. Reg. 62,011, 62,014 (Oct. 31, 2003), available at <http://www.gpo.gov/fdsys/pkg/FR-2003-10-31/pdf/03-27537.pdf>.

¹⁴¹ Class 9 Proponents have also asserted that an exemption is needed to bring the U.S. “into compliance with the Marrakesh Treaty” adopted by the World Intellectual Property Organization. *AFB Class 9 Comments* at 4. NTIA takes no position on this argument and believes that proponents and supporters of this class have presented enough evidence in the record to meet the statutory requirements for an exemption during the next three year period.

¹⁴² See *AFB Class 9 Comments* at 4-9 (providing an example of various TPMs embedded in e-books such as Apple’s FairPlay DRM System, Kindle Format, and Adobe Content Server).

devices or applications to gain access to e-books or the literary content therein.¹⁴³ Moreover, NTIA, the Copyright Office, and the Librarian of Congress have previously supported exemptions that were substantially similar to this proposal.¹⁴⁴ The conclusion that the proposed use is noninfringing continues to be supported by current law,¹⁴⁵ the legislative history of the current Copyright Act,¹⁴⁶ and legal precedent.¹⁴⁷ Lastly, NTIA notes that no party filed comments opposing the renewal of the current exemption.¹⁴⁸

NTIA also supports renewal of the current exemption because the record indicates that there continues to be a need to convert materials to accessible formats.¹⁴⁹ More notably, the record contains many clear and specific examples of the many ways disabled users and authorized

¹⁴³ See, e.g., *AFB Class 9 Comments* at 8-10 (discussing how TPMs in e-books generally restrict text-to-speech screen readers and refreshable Braille displays from accessing the literary work); *Class 9 Comments of iFixit (iFixit Class 9 Comments)* at 1-2, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_iFixit_Class09.pdf (noting that “DRM on legally purchased e-books blocks the ability of owners to access the book through text-to-speech programs – many of which come preinstalled on e-readers” and that “[o]nly 1% of published books are available in braille”); *Comments of the Association of American Publishers* at 1, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_AAP_Class09.pdf (access controls can “prevent the use of screen readers for the print-disabled, and if no other format is available, can effectively block access to digital print content”).

¹⁴⁴ See *2012 NTIA Letter* 4-5; *2012 Register’s Recommendation* at 21-23; *2012 Final Rule* at 25262-63.

¹⁴⁵ See 17 U.S.C. § 121(a) (2012).

¹⁴⁶ The House Report on the Copyright Act of 1976 cites the making “of copies or phonorecords of works in the special forms needed for the use of blind persons” as a “special instance illustrating the application of the fair use doctrine...” See H.R. Rep. No. 94-1476, at 73 (1976), reprinted in 1976 U.S.C.C.A.N. 5659, 5686-87.

¹⁴⁷ See, e.g., *Sony Corp. of America v. Universal City Studios Inc.*, 464 U.S. 417, 455 n.40 (1984); *Author’s Guild, Inc. v. Publications Int’l Ltd.*, 996 F.2d 1366, 1375 (2d Cir. 2014) (noting that the Chafee Amendment, codified at 17 U.S.C. § 121, “illustrates Congress’s intent that copyright law make appropriate accommodations for the blind and print disabled”).

¹⁴⁸ There was one filing submitted by 121AuthEnt.org during the designated round for those who oppose the adoption of a proposed exemption; however, this filing was simply to clarify a claim made in the *AFB Class 9 Comments* and the author made it explicitly clear that he was “not opposed to granting” this exemption. See *Class 9 Comments of 121AuthEnt.org* at 4, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%209/121AuthEnt_class09_1201_2014.pdf.

¹⁴⁹ See, e.g., *Class 9 Combined Comments* at 15, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/EFF_merged_shortform_comments_class09.pdf (“A lot of professors encouraged and often required their students to use scholarly articles and journals to do research. I liked the concept of an online library database, because I assumed that such material would be accessible to me simply because it was available electronically. I was incorrect in this assumption, however, because much of the material I needed to access was in inaccessible PDFs”); *Class 9 Combined Comments* at 29 (“Blind students seeking an education are running into the issue that their textbooks are not accessible; they cannot access their course materials and therefore cannot function alongside their sighted peers in the classroom”); *iFixit Class 9 Comments* at 4-6; *Class 9 Comments of the Music Library Association* at 1, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_MLA_Class09.pdf.

entities are utilizing this exemption as intended and thus making literary works more accessible with assistive technologies.¹⁵⁰

For all these reasons, NTIA supports renewing the current exemption, without change:

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.

2. Space Shifting and Format Shifting (Class 10)

During the initial petition phase of this proceeding, Christopher Meadows proposed an exemption to circumvent access controls protecting lawfully-purchased e-books “in order to back them up, read them on other e-book platforms, or otherwise make section 107 fair use of the material.”¹⁵¹ Essentially, this proposed class would serve as an analogue to proposed Class 8, which addresses space shifting of audiovisual works. This proponent, however, did not follow up with a fully supported request for an exemption at the second stage of submissions.

As NTIA discussed in its recommendation for space shifting in the audiovisual context, NTIA is open to this type of exemption in principle. The legal arguments for and against the legality of noncommercial space shifting are likely the same for literary and audiovisual works. We further suspect that the harms to consumers from the prohibition against circumvention are similar in both cases. Unfortunately, proponents have not submitted sufficient evidence on the record in this proceeding to support an exemption. The original petitioner notes that “over the last few years, a number of e-book stores have ceased operations,” and as a result, “consumers who had purchased e-books from those businesses lost access to the books they had purchased.”

¹⁵⁰ See, e.g., *AFB Class 9 Comments* at Appendix A (submission by a University of Colorado official that provides “accessible versions of textbooks and other required course materials to students with disabilities” under a structured process and asserts such students will suffer “several harms” if this exemption is not renewed); *AFB Class 9 Comments* at Appendix B (various letters depicting the challenges that blind students face in obtaining accessible works).

¹⁵¹ See Initial Petition of Christopher Meadows at 1, Docket No. 2014-07, available at http://copyright.gov/1201/2014/petitions/Meadows_Christopher_1201_Initial_Submission_2014.pdf.

He further laments that, due to TPMs, consumers are unable to move among different e-reader platforms without losing or re-purchasing the titles in their personal libraries.¹⁵² Separately, proponent Rachel Englander reports that she has “been in the position of having to purchase multiple copies of the same items, due to computer failure and restrictive DRM that prevents a backup being made.”¹⁵³ Finally, the Music Library Association argues that “as e-book readers and file formats become obsolete, and as permissible under Section 108, music librarians need to create preservation copies of textual works.”¹⁵⁴ However, neither the Music Library Association nor any other party specifically proposed and supported an exemption tailored towards libraries for Section 108 purposes.

Absent a more complete evidentiary record, NTIA cannot recommend an exemption at this time for space shifting of literary works.

C. Unlocking: Software Interoperability with Networks (Classes 11-15)

Over the past several years, NTIA has become increasingly concerned with the wireless industry practice of locking devices to particular networks. The use of technology to deter wireless device owners from moving among wireless carriers—and claiming that the technology is an access control under the DMCA—is one of the earliest and most enduring examples of Section 1201 being used to further interests that are unrelated to copyright protection. As NTIA have noted in other proceedings, the practice of locking wireless devices has “forced consumers to acquire new devices when they switch operators, unnecessarily increasing the cost of the new service,” which “not only harms consumers, but also creates an artificial barrier within the market that limits device portability, hindering competition among providers.” Furthermore, “locked wireless devices also hinder the market for used or previously deactivated devices.”¹⁵⁵

NTIA’s previous engagement on this important issue of consumer choice and marketplace competition did not end with the conclusion of the 2012 rulemaking. During that proceeding, NTIA recommended, based on both the record at hand and its own subject matter expertise, that the Librarian renew the exemption for unlocking handsets and expand it to include all wireless devices.¹⁵⁶ Following the Librarian’s decision to instead limit the exemption to handsets

¹⁵² *Id.*

¹⁵³ Class 10 Comments of Rachel Englander at 1, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_Englander_Class10.pdf.

¹⁵⁴ Class 10 Comments of Music Library Association at 1, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_MLA_Class10.pdf.

¹⁵⁵ *See* In the Matter of Amendment of Part 20 of the Commission’s Rules and Regulations to Require Certain Providers of Commercial Mobile Radio Services to Unlock Wireless Devices Upon Request, *Petition for Rulemaking of the National Telecommunications and Information Administration*, (NTIA Petition) at 10-11, *available at* http://www.ntia.doc.gov/files/ntia/publications/ntia_mobile_devices_unlocking_petition_09172013.pdf.

¹⁵⁶ *See* 2012 NTIA Letter at 18.

originally sold on or before January 26, 2013,¹⁵⁷ over 114,000 concerned Americans petitioned the White House to take action to ensure the legality of unlocking wireless devices.¹⁵⁸ In its response to this petition, the White House noted that “the DMCA exception process is a rigid and imperfect fit for this telecommunications issue,” and directed NTIA to formally engage with the Federal Communications Commission (FCC) to address unlocking as a matter of telecommunications policy.¹⁵⁹

Following this White House directive, NTIA petitioned the FCC to initiate a rulemaking that would require wireless carriers to unlock wireless devices upon request—thereby reducing the need for users to attempt unlocking through circumvention.¹⁶⁰ NTIA proposed amending Part 20 of the FCC’s Rules and Regulations to require that, upon request, any wireless carrier “shall, without fee, unlock any wireless device furnished to that customer or successor by the [carrier], an affiliate, or an authorized agent.”¹⁶¹ This effort helped precipitate a voluntary agreement between the FCC and major wireless carriers that enables consumers to have their devices unlocked in many—though not all—of the situations contemplated in NTIA’s petition.¹⁶² This agreement is important for bolstering real consumer choice and competition in the wireless market because it provides a much more accessible and reliable means of enabling device portability. Rather than taking on the technically challenging and risky task of circumventing TPMs that prevent changing carrier settings, users can now in many cases simply request that the carrier remove any such barriers through supported means.

While NTIA welcomes the adoption by certain carriers of more permissive unlocking policies, an exemption under Section 1201 remains an important failsafe that empowers Americans to take matters into their own hands when wireless carriers refuse (or lack the means¹⁶³) to unlock particular devices. The thousands of people who have written to the

¹⁵⁷ See *2012 Final Rule* at 65,278 (Issuing an unlocking exemption for handsets “originally acquired from the operator of a wireless telecommunications network or retailer no later than ninety days after the effective date of this exemption.”).

¹⁵⁸ *Making Unlocking Cell Phones Legal*, Jan. 24, 2013, (last visited Sep. 15, 2015), available at <https://petitions.whitehouse.gov/petition/make-unlocking-cell-phones-legal>.

¹⁵⁹ *It’s Time to Legalize Cell Phone Unlocking*, Official White House Response to Make Unlocking Cell Phones Legal, Mar. 4, 2013, (last visited Sept. 15, 2015) available at <https://petitions.whitehouse.gov/response/its-time-legalize-cell-phone-unlocking>.

¹⁶⁰ *NTIA Petition* at 3-4.

¹⁶¹ *Id.* at 4.

¹⁶² See *Cell Phone Unlocking*, Federal Communications Commission (last visited Sept. 8, 2015), available at <https://www.fcc.gov/encyclopedia/cell-phone-unlocking> (this site gives a summary of the voluntary agreement); see also *Consumer Code for Wireless Service (CTIA Voluntary Code)*, CTIA The Wireless Association (last visited Sept. 8, 2015), available at <http://www.ctia.org/policy-initiatives/voluntary-guidelines/consumer-code-for-wireless-service>.

¹⁶³ For example, Sprint notes that “many devices that have been manufactured for Sprint simply are not [domestic SIM unlock]-capable,” because “prior to the voluntary commitment... carriers were not required to, and many carriers did not, develop their devices to be capable of being unlocked.” See *FAQs About Unlocking Your Sprint*

Copyright Office in support of unlocking exemptions for handsets, tablets, and other wireless devices make clear that they continue to require the ability to circumvent in a variety of cases. For example, Howard Chu notes in his comment that, for business reasons, he is “frequently spending enough time in foreign countries that it’s advantageous to buy a local SIM card in that country instead of roaming on [his] US phone plan.”¹⁶⁴ Even among those carriers that adhere to the voluntary agreement on device unlocking, some will decline to unlock devices for international travel if the device is subject to an ongoing service commitment or installment plan.¹⁶⁵ Separately, Tammy Furloni highlights the harmful economic and environmental consequences of the prohibition against circumventing access controls that prevent unlocking. She points out the significant barrier erected when, “unless [she wants] to spend \$500 or \$600 on a new phone, [she] can’t change carriers,” and further notes that “being unable to switch carriers makes for extra waste.”¹⁶⁶

Whether due to policies or technical limitations, it is clear that an unlocking exemption remains necessary in many situations. Without one, many users continue to face artificial restraints on their ability to move among wireless carriers, which is why, as NTIA previously stated in its 2012 consultation letter, “NTIA does not support the notion that it is an appropriate alternative” to circumvention “for a current device owner to be required to purchase another device to switch carriers.”¹⁶⁷ More fundamentally, this is a matter with little relation to copyright protection and a strong grounding in basic consumer rights. Jack Dintruff captures commenter sentiment succinctly when he expresses “that [his] rights as a consumer are being taken away... when regulators designate what [he cannot] do with the hardware [he] purchased.”¹⁶⁸

In this rulemaking, proponents seek the ability to circumvent TPMs on a broader range of devices in order to enable interoperability with different wireless networks. The most significant proposals for expanding the unlocking exemption would cover several classes of devices (including handsets,¹⁶⁹ tablets,¹⁷⁰ wearables,¹⁷¹ mobile hotspots,¹⁷² and others¹⁷³) or all wireless

Device, Sprint (last visited Sept. 15, 2015), *available at* http://support.sprint.com/support/article/FAQs_about_unlocking_your_Sprint_device/7a3bf815-cfed-4a56-925a-7a187d1c6637#1/.

¹⁶⁴ See Class 11 Combined Comments at 902, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/reply-comments-050115/class%208/EFF_merged_shortform_comments_class08.pdf.

¹⁶⁵ For example, AT&T states that unlocking requests will only be honored if “all the device’s service commitments and installment plans are completed, and all early termination fees are paid in full.” See General Requirements for All Unlock Requests, AT&T, <https://www.att.com/deviceunlock> (last visited Sept. 15, 2015).

¹⁶⁶ *Class 11 Combined Comments* at 2124.

¹⁶⁷ *2012 NTIA Letter* at 17.

¹⁶⁸ *Class 11 Combined Comments* at 929.

¹⁶⁹ Class 11 Comments of the Competitive Carriers Association (*CCA Class 11 Comments*) at 1, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_CCA_Class11.pdf.

devices generally.¹⁷⁴ As in 2012, NTIA continues to believe that “the line that distinguishes a mobile phone from other wireless devices is increasingly disappearing.”¹⁷⁵ In fact, there are more reports in the record in this proceeding of a large range of wireless devices that may be locked to carrier networks, including mobile phones, tablets, and wearables. Therefore, NTIA reiterates our 2012 position that this exemption should be extended to all wireless devices that connect to a wireless network offering telecommunications and/or information services. In addition to the substantial record in support of exemptions for a number of devices, the Copyright Office has long taken the view that “a ‘particular class of copyrighted works’ must relate primarily to attributes of the copyrighted works themselves and not to factors that are external to the works, *e.g.*, the material objects on which they are fixed or the particular technology employed on the works,” as this document notes above.¹⁷⁶ While exemptions *may* be further refined based on the record, it is clear that exemptions should be based on the works at issue, and not the screen size or form factor of the devices on which they are contained. Due to the broad record in this proceeding, as well as the rapid pace of innovation in this space, NTIA urges adoption of an exemption that covers the full range of wireless devices.

Proponents have offered detailed evidence as to the need for an unlocking exemption, as well as its noninfringing nature. There is evidence in the record for each proposed class that devices are routinely locked,¹⁷⁷ and that carriers often are resistant to supplying unlocking codes or have policies that restrict unlocking indirectly, highlighting the need for consumers to be able to legally unlock their devices themselves.¹⁷⁸ Regarding a fair use determination, there has been evidence that the effect on the market has been positive after unlocking became legal, and that

¹⁷⁰ Class 12 Comments of iFixit at 1, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_iFixit_Class12.pdf.

¹⁷¹ Class 14 Comments of the Competitive Carriers Association (*CCA Class 14 Comments*) at 1, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_CCA_Class14.pdf.

¹⁷² Class 13 Comments of the Competitive Carriers Association (*CCA Class 13 Comments*) at 1, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_CCA_Class13.pdf.

¹⁷³ Class 15 Comments of iFixit at 1, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_iFixit_Class15.pdf.

¹⁷⁴ Class 12 Comments of Consumers Union at 2, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_iFixit_Class12.pdf.

¹⁷⁵ *See 2012 NTIA Letter* at 19.

¹⁷⁶ *2000 Final Rule* at 64,562.

¹⁷⁷ *See* Class 15 Comments of the Competitive Carriers Association (*CCA Class 15 Comments*) at 4, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_CCA_Class15.pdf; *see also* *CCA Class 14 Comments* at 4; Class 12 Comments of Competitive Carriers Association (*CCA Class 12 Comments*) at 4, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_CCA_Class12.pdf.

¹⁷⁸ *CCA Class 12 Comments* at 8; *CU Class 12 Comments* at 20.

when the Librarian limited the exemption, devices that could not be unlocked lost resale value.¹⁷⁹ All other factors are either neutral or favor the proponents in a fair use determination.¹⁸⁰ Proponents further make the case that, to the extent that a derivative work may be created in the course of unlocking, such action falls within the Section 117(a)(1) exception because “the changes being made to the copyrighted work are the same ones that need to be made by the underlying carrier in order for the [device] to operate properly” on a different network.¹⁸¹

Three parties submitted comments in opposition to the proposed unlocking exemptions, including TracFone,¹⁸² General Motors, and the Alliance of Automobile Manufacturers. Their comments are directed at protecting their interests in any granted exemptions, rather than complete opposition to any exemptions for device unlocking.¹⁸³ Of the three, only TracFone raises any concern related to copyright infringement, partly in the context of asserting that proponents haven’t proven that unlocking is always noninfringing.¹⁸⁴ Other opponents rely overwhelmingly on raising concerns with no basis in copyright law, such as vehicle emissions and safety standards. For example, General Motors asserts that “the TPMs that Proponents seek to circumvent are the same TPMs that protect general vehicle functionality, ensure vehicle safety and cybersecurity, protect key consumer privacy interests, and enable compliance with federal

¹⁷⁹ *CU Class 12 Comments* at 15-19.

¹⁸⁰ In support of their argument, proponents note that (1) The purpose of the use is to allow the lawful owner of the device to connect to a wireless network of their choice, which is noninfringing. (2) When a device is first made, its preferred roaming list variables have not been set, and changing those variables makes the device compatible with a given network. In order to unlock a phone, one changes the variables, and therefore this change is intended by the manufacturer. (3) The amount of code “used in an altered state is extremely small” compared to a device’s operating system as a whole. See *CCA Class 15 Comments* at 5; *CCA Class 14 Comments* at 5; see also *Class 12 Reply Comments of the Consumers Union* at 9, Docket No. 2014-07, available at http://copyright.gov/1201/2015/reply-comments-050115/class%2012/ReplyCommentsConsumersUnion_Class12.pdf; *Class 12 Comments of the Institute of Scrap Recycling Industries (ISRI Class 12 Comments)* at 9, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_ISRI_Class12.pdf.

¹⁸¹ *CCA Class 11 Comments* at 5.

¹⁸² We note that, in reply comments, TracFone and the Competitive Carriers Association offered compromise exemption language that TracFone would find acceptable. However, the language offered would, in NTIA’s view, render an exemption unacceptably narrow by restricting it to situations where the terms of “any subsidy, discount, installment plan, lease, rebate or other incentive program” have been met in full. See *Joint Class 11 Reply Comments of the Competitive Carriers Association and TracFone Wireless, Inc.* at 2, Docket No. 2014-07, available at http://copyright.gov/1201/2015/reply-comments-050115/class%2011/ReplyCommentsCCAandTracfone_Class11.pdf.

¹⁸³ For example, the Alliance of Automakers noted in part that “if any exemption is recommended in this area, it should not extend to motor vehicles.” See *Class 13 Comments of Alliance of Automobile Manufacturers* at 1, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%2013/Alliance_of_Automobile_Manufacturers_class13_1201_2014.pdf.

¹⁸⁴ *Class 11 Comments of TracFone (TracFone Class 11 Comments)* at 10, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%2011/TracFone_Wireless_class11_1201_2014.pdf.

safety and emissions requirements.”¹⁸⁵ As discussed in the earlier portion of this document, in no case is the prohibition against circumvention an appropriate or effective tool for furthering these non-copyright interests.

Unlike most wireless carriers, TracFone develops extensive custom software for use with the mobile devices it sells, making the company uniquely positioned in this proceeding to express concerns about copyright issues.¹⁸⁶ However, TracFone offers no evidence of harm resulting from an exemption that has been in place, with only brief interruption, since 2006. Indeed, TracFone’s own comments detail the many successful lawsuits it has brought against traffickers, the vast majority of which were litigated while the unlocking exemption was in place.¹⁸⁷ This supports the proposition that enabling owners to unlock their devices and use them with the carriers of their choice will not interfere with wireless carriers pursuing traffickers.

TracFone’s history with the unlocking issue serves as a useful example of the continuing need for an exemption despite the voluntary industry agreement. Until recently, the company declined to participate in the wireless industry’s voluntary agreement on mobile device unlocking.¹⁸⁸ This was despite the fact that the FCC requires each wireless carrier to “demonstrate that it will satisfy applicable consumer protection and service quality standards” in order to be eligible for Lifeline subsidies—a requirement that can be satisfied through compliance with an industry code that includes the voluntary unlocking agreement.¹⁸⁹ Since it participates in the Lifeline program, TracFone’s failure to implement a broad unlocking policy led to an FCC investigation, in which it “found that TracFone violated agency rules by improperly certifying that it would unlock phones for its customers enrolled in the FCC’s Lifeline program.” As part of the settlement, TracFone “has agreed to transition all its phones to be unlockable,” which will eventually allow all customers (Lifeline or otherwise) to move to other networks.¹⁹⁰

¹⁸⁵ Class 13 Comments of General Motors (*GM Class 13 Comments*) at 4, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%2013/General_Motors_class13_1201_2014.pdf.

¹⁸⁶ TracFone explains that “many TracFone handsets include customized software and firmware that enable the devices to operate on carriers with which TracFone has contracted to provide networks services to its customers, and to implement TracFone’s pay-as-you-go business model.” See *TracFone Class 11 Comments* at 4.

¹⁸⁷ *TracFone Class 11 Comments* at 19-23. TracFone notes that “from 2005 to the present, TracFone has filed lawsuits against 208 phone trafficker defendants in federal courts across the United States, and has obtained 74 final judgments and permanent injunctions in its favor.” *Id.* at 6.

¹⁸⁸ The voluntary agreement is part of the CTIA Code of Conduct. See *CTIA Voluntary Code* at 1. As listed on that page, TracFone is not a signatory to the CTIA Code of Conduct, though agreeing to the entirety of the Code is not a requirement for implementing the voluntary agreement.

¹⁸⁹ 47 C.F.R. § 54.202(a)(3).

¹⁹⁰ Press Release, FCC Reaches Agreement with TracFone to Unlock Mobile Phones & Provide Other Consumer Benefits: Settlement Brings Benefits to Millions of Consumers, (July 1, 2015), available at <https://www.fcc.gov/document/fcc-reaches-agreement-tracfone-unlock-mobile-phones-0>.

Having analyzed the record, NTIA is persuaded that renewing an exemption for network interoperability purposes will not adversely affect the market value of copyrighted works, and will provide relief from the harm proponents have demonstrated. Accordingly, NTIA suggests the same language we proposed during the 2012 proceeding:

Computer programs, in the form of firmware or software (including data used by those programs) that enable used wireless devices to connect to a wireless network that offers telecommunications and/or information services, where circumvention is initiated by the owner of the copy of the computer program 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.

NTIA detailed the language changes it proposed in its 2012 consultation letter, and we continue to support the same language choices.¹⁹¹ To provide further clarity in the context of this proceeding, NTIA intends to include at minimum mobile phones (class 11), tablets (class 12), mobile connectivity devices (class 13), wearable devices (class 14), and future devices contemplated as “consumer machines” (class 15) within the scope of “wireless devices.” The 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. We thus urge against enumerating a list of covered devices that will inevitably prove ambiguous or obsolete within the next three years. Finally, NTIA points out that, in a hearing, witnesses acknowledged that unlocking a wireless radio embedded in a motor vehicle is “not possible at the moment” and is not achievable without destroying the vehicle (“or even in the process of destroying your car, I’m not sure it’s possible”).¹⁹² Because the wireless equipment in motor vehicles may serve substantially different purposes from that in other devices, and in light of both the current technical infeasibility and lack of desire on the record to unlock a vehicle’s wireless equipment, NTIA would not oppose the exclusion of wireless radios embedded in vehicles from the exemption at this time—though such an exclusion also does not appear to be necessary.

D. Jailbreaking: Software Interoperability with Software

1. Mobile Devices (Classes 16-18)

Proponents seek the ability to circumvent access controls in a variety of devices in order to enable the interoperability and installation of lawfully obtained third-party software.¹⁹³ Exemptions enabling this practice, commonly referred to as “jailbreaking” (or “rooting” for devices that run the Android operating system), are requested for the following:

¹⁹¹ See 2012 NTIA Letter at 18-20.

¹⁹² May 21 Hearing Transcript at 39. In the hearing, proponents largely disclaimed interest in including vehicles in this proposed exemption.

¹⁹³ NTIA notes that jailbreaking a device may also allow for the removal of unwanted software.

- Wireless telephone handsets¹⁹⁴
- All-purpose mobile computing devices¹⁹⁵
- Dedicated e-book readers¹⁹⁶

In the previous rulemaking, the Librarian granted an exemption after NTIA and the Copyright Office concluded that modifying a mobile phone's firmware to run lawfully-acquired software is noninfringing.¹⁹⁷ The current record shows that the marketplace for mobile devices has not substantially changed from three years ago; specifically, most mobile devices continue to be sold or distributed with access controls that restrict the installation of third party applications or removal of unwanted software.¹⁹⁸ As the Register noted in 2010, "[w]hile a copyright owner might try to restrict the programs that can be run on a particular operating system, copyright law is not the vehicle for imposition of such restrictions, and other areas of the law, such as antitrust, might apply. It does not and should not infringe any of the exclusive rights 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."¹⁹⁹ In addition, the record contains extensive anecdotal evidence demonstrating the noninfringing uses that can be accomplished after jailbreaking.²⁰⁰ Therefore, NTIA again supports this exemption and, as discussed below, advocates the inclusion of a greater spectrum of mobile devices consistent with the record.

¹⁹⁴ See generally Class 16 Comments of the Electronic Frontier Foundation (*EFF Class 16 Comments*), Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_EFF_Class16.pdf; Class 16 Comments of Jay Freeman (*Freeman Class 16 Comments*) Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_Freeman_Class16.pdf; Class 16 Comments of New Media Rights (*NMR Class 16 Comments*), Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_New_Media_Rights_Class16.pdf.

¹⁹⁵ See generally Class 17 Comments of the Electronic Frontier Foundation (*EFF Class 17 Comments*), Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_EFF_Class17.pdf; Class 17 Comments of Jay Freeman (*Freeman Class 17 Comments*), Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_Freeman_Class17.pdf; Class 17 Comments of New Media Rights (*NMR Class 17 Comments*), Docket No. 2014-07, http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_NewMediaRights_Class17.pdf.

¹⁹⁶ See Class 18 Comments of Jay Freeman (*Freeman Class 18 Comments*), Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_Freeman_Class18.pdf.

¹⁹⁷ See 2012 *Final Rule* at 65,278; see also 2012 *NTIA Letter* at 11-13; 2012 *Register of Copyrights Recommendation* at 79.

¹⁹⁸ *EFF Class 16 Comments* at 4-6 (discussing various access controls found in Apple and Android devices); *EFF Class 17 Comments* at 4-6 (discussing various access controls on mobile operating systems); *Freeman Class 18 Comments* at 4-6.

¹⁹⁹ 2010 *Register of Copyrights Recommendation* at 96-97.

²⁰⁰ See, e.g., Class 16 Comments of Blinky X , Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_Blinky_X_Class16.pdf (blind iPhone owner who jailbreaks to install an application that has the ability to tell the time by a series of vibrations, and

NTIA notes that that the proposed exemption would also aid in the repair of mobile devices. In those circumstances, circumvention is needed because during the repair process one may have to “downgrade a version [or]... install a specialized repair [app].”²⁰¹ In the case of diagnosis, there may be a need to “get through the operating system to access some of the remote access controls.”²⁰² In many ways, this is similar to digital gaming consoles, where circumvention is sometimes needed to complete a repair successfully.

The record supports expansion of this exemption to include jailbreaking of mobile computing devices generally. The expansion from cell phones to mobile devices generally stems from the fact that, regardless of a device’s particular form factor, the works and TPMs at issue are strikingly similar and many times identical.²⁰³ Different types of devices are increasingly sold with virtually identical operating systems or variations thereof. For instance, although the current exemption is crafted for “wireless telephone handsets,” one of the proponents convincingly demonstrated in a hearing that many Apple mobile devices, such as the iPad, iPod Touch, and iPhone, operate using Apple’s iOS.²⁰⁴ Thus, it is increasingly difficult to draw a distinction between each device for purposes of this exemption, and therefore it should apply to all of them regardless of size or form factor.

to install another application that allows the activation of the springboard, Siri, the app switcher and the spotlight search simply by tapping sections of the touch screen rather than the button itself); Class 16 Comments of Eli Cantarero, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_Cantarero_Class16.pdf (disabled Veteran describing various apps for specific needs such as to increase font sizes, icon sizes, or for the speaking of all notifications in earphones); *NMR Class 16 Comments* at 18-25 (describing new technologies and methods of self-help that jailbreaking makes available to consumers and the ability to fix software vulnerabilities); Class 16 Comments of Jeffrey Philip Roddy, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_Roddy_Class16.pdf (discussing how his phone can be enhanced with third-party applications after jailbreaking); Class 16 Comments of Micah Ross, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_MRoss_Class16.pdf (explaining that “[t]he iPhone screen uses very bright blue light for its display, and that has always been hard on my eyes. iOS doesn’t have anything to fix the lighting, but Jailbreaking my phone lets me change the lighting to more of a candle-light like display”); Class 17 Comments of Nathan Scandella, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_Scandella_Class17.pdf (app developer that jailbreaks to allow software testing).

²⁰¹ *May 21 Hearing Transcript* at 90.

²⁰² *Id.*

²⁰³ The record shows that the access controls for wireless telephone handsets, tablets, and other mobile devices are nearly identical and many times the same. See generally *EFF Class 16 Comments* at 4-6; *EFF Class 17 Comments* at 4-6; *Freeman Class 16 Comments* at 4-5; *Freeman Class 17 Comments* at 4-5.

²⁰⁴ See *May 21 Hearing Transcript* at 56-59 (In the context of the various Apple mobile devices, Mr. Freeman noted that “it becomes very difficult to really appreciate the exact boundaries that delineate this particular sequence of small, black, rectangular touchscreen devices” and that “[i]f I hold an Apple watch and hold it next to what is an original iPhone, it’s, again, just another smaller device, a small, rectangular device, flat with a touchscreen.”).

Similar to the prior discussion on unlocking, the statutory factors weigh in favor of proponents in a fair use determination.²⁰⁵ In particular, there continues to be evidence to indicate that the mobile applications market has thrived despite the existence of an exemption for over five years.²⁰⁶ In today's digital economy, consumer demand for mobile applications has not waned; to the contrary, as of June of last year, more than 75 billion mobile applications had been downloaded from the Apple App Store alone.²⁰⁷

NTIA also notes that, when compared to prior rulemakings, opposition to an exemption for software interoperability purposes has drastically diminished. One of the few opponents—the BSA—opposes this class because proponents have not “proffered a clearly defined class of works.”²⁰⁸ This claim is unsupported by the record. Proponents have clearly described the classes of work, in this case, computer programs in mobile devices. BSA further asserts that opponents offer “no credible means to distinguish between tablets and laptops,”²⁰⁹ but for purposes of this exemption, consumers need not make this distinction for two reasons. First, laptops are not typically subject to the TPMs found in mobile devices that effectively control installation or removal of third-party applications.²¹⁰ Second, there is no evidence in the record that proponents are seeking to circumvent access controls on laptops. BSA also states that proponents have not met their burden of proof because they have conceded that “consumers may purchase all-purpose mobile devices that do not prevent installation of third-party software applications.”²¹¹ NTIA continues to reject the idea that the availability for purchase of another device constitutes a viable alternative to circumvention. Instead, the relevant inquiry is whether owners of devices can make noninfringing use of copyrighted works without encountering significant barriers (e.g., prohibitive costs). In sum, opponents of this class do not provide an

²⁰⁵ See generally *EFF Class 16 Comments* at 7-15; *EFF Class 17 Comments* at 7-15. NTIA notes that there is no evidence in the record that would illustrate, with sufficient specificity, how the installation and/or removal of third-party software would not fall within the fair use doctrine or otherwise be an infringing action.

²⁰⁶ See Niall McCarthy, *Mobile App Usage By The Numbers [Infographic]*, *Forbes* (Oct. 29, 2014, 9:00 AM), <http://www.forbes.com/sites/niallmccarthy/2014/10/29/mobile-app-usage-by-the-numbers-infographic/>; see also Anne Lu, *6.1 billion smartphone users by 2020: What it means for mobile apps*, *International Business Times* (Aug. 29, 2015, 11:37 PM), <http://www.ibtimes.com.au/61-billion-smartphone-users-2020-what-it-means-mobile-apps-1458986>.

²⁰⁷ Statistics and facts about Mobile App Usage, Statista, <http://www.statista.com/topics/1002/mobile-app-usage/> (last visited Aug. 10, 2015) (As of June 2014, more than 75 billion mobile apps had been downloaded from the Apple App Store alone)

²⁰⁸ See *Class 17 Comments of BSA – The Software Alliance (BSA Class 17 Comments)* at 1, Docket No. 2014-07, available at [http://copyright.gov/1201/2015/comments-032715/class%2017/BSA The Software Alliance class17 1201 2014.pdf](http://copyright.gov/1201/2015/comments-032715/class%2017/BSA%20The%20Software%20Alliance%20class17%201201%202014.pdf).

²⁰⁹ *BSA Class 17 Comments* at 1-2.

²¹⁰ *EFF Class 17 Comments* at 3-4 (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”).

²¹¹ *BSA Class 17 Comments* at 2.

alternative legal theory or cite viable alternatives to circumvention that would support a different conclusion from the last rulemaking.

The other opponents of jailbreaking classes, General Motors (GM) and the Alliance of Automobile Manufacturers (AAM), are mainly concerned with the applicability of possible exemptions to vehicles.²¹² However, proponents have made it clear that they are not seeking circumvention of access controls in vehicles.²¹³ In addition, the record does not indicate that access controls in vehicles need to be circumvented for software interoperability purposes. Accordingly, NTIA does not intend to include vehicles in this exemption. However, it is possible that an exemption for vehicles may be proposed in a future proceeding, given the rapid advance of technology in that industry. NTIA therefore reiterates its call to manufacturers to be cognizant of the purpose for which a particular TPM is implemented.

As discussed, the Copyright Office should recommend a jailbreaking exemption that includes “mobile computing devices” generally, and should move away from the previous practice of enumerating specific types of devices. Accordingly, NTIA recommends the following exemption:

Computer programs that enable mobile computing devices 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.

2. Video Game Consoles (Class 19)

During the initial petition stage, a proponent sought an exemption to allow the circumvention of access controls in gaming devices such as “Nintendo’s Wii U, Sony’s Play Station 4, Microsoft’s Xbox One and home media devices like Apple TV” to allow installation of third-party applications.²¹⁴ However, the record indicates that the original proponent did not pursue this exemption any further; instead, iFixit provided the majority of evidence for this proposed class, focusing almost exclusively on an exemption to allow the circumvention of access controls

²¹² See Class 17 Comments of the Alliance of Automobile Manufacturers at 1, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-032715/class%2017/Alliance_of_Automobile_Manufacturers_class17_1201_2014.pdf; see also Class 17 Comments of General Motors, LLC at 3-4, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-032715/class%2017/General_Motors_class17_1201_2014.pdf; *May 21 Hearing Transcript* at 72 (Mr. Lightsey from GM stated that “[r]equiring the jailbreaking of vehicle telematics and communication systems would have a negative impact on vehicle and consumer safety, security and privacy, as well as on emissions and regulatory compliance and could have a chilling effect on future development in the area.”).

²¹³ *May 21 Hearing Transcript* at 53, 72 (Mr. Stoltz from EFF asserted that this proposal “does not include vehicle electronics” and that “Class 17 simply doesn’t encompass vehicles”).

²¹⁴ See Initial Petition of Maneesh Pangasa, Docket No. 2014-07, *available at* http://copyright.gov/1201/2014/petitions/Pangasa_Maneesh_2_1201_Initial_Submission_2014.pdf.

in gaming consoles for the purpose of repairing console hardware.²¹⁵ A similar exemption for this purpose was proposed in the previous rulemaking.²¹⁶ NTIA then recommended that the Librarian adopt an exemption to allow circumvention of access controls only for console repair.²¹⁷ NTIA did not recommend a broader exemption for software interoperability due to an insufficient record.²¹⁸ For simplicity purposes in this proceeding, NTIA will discuss software and hardware interoperability issues separately.

Software Interoperability

The arguments for and against an exemption for software interoperability are nearly identical to the previous rulemaking. iFixit states that “[m]odifying the software on a game console isn’t necessarily undertaken as part of a ploy to pirate games” and that denying this exemption “only handicaps the users who are jailbreaking to expand the functionality of their machines... punishes the researchers... and penalizes the modders who want a little more choice about how their consoles perform.”²¹⁹ iFixit also argues that circumvention of access controls in gaming consoles is noninfringing just like the Copyright Office has recognized in mobile phones.²²⁰

The Entertainment Software Association (ESA) opposes this exemption because the record “fails to support a finding that the inability to circumvent access controls on video game consoles has, or over the course of the next three years likely would have, a substantial adverse impact on the ability to make noninfringing uses.”²²¹ In addition, ESA claims that there is substantial evidence in the record that console jailbreaking “leads to a higher level of infringing activity.”²²² In support of these claims, ESA has introduced exhibits that demonstrate the wide availability of

²¹⁵ See Class 19 Comments of iFixit (*iFixit Class 19 Comments*), Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_iFixit_Class19.pdf; see also *May 20 Transcript Hearing* at 285 (“We (iFixit) are interested in an exemption that would allow us to repair these products (referring to gaming consoles)”; *id.* at 288 (Mr. Kyle Wiens from iFixit noting that his “primary interest is in repair.”).

²¹⁶ See 2012 NTIA Letter at 5-8.

²¹⁷ See *id.* at 8 (In 2012, NTIA proposed the following exemption “Computer programs that enable video game console hardware to operate with the console operating system, when circumvention is initiated by the owner of the console for the purpose of repairing or replacing malfunctioning hardware, for systems that are obsolete or no longer covered by manufacturer warranty”).

²¹⁸ See *id.* at 6 (Specifically, NTIA found that “the record [was] not clear that an exemption [was] warranted for enabling interoperability with unauthorized applications or for installing an unauthorized operating system.”).

²¹⁹ *iFixit Class 19 Comments* at 3.

²²⁰ *Id.* at 3-4.

²²¹ See Class 19 Comments of the Entertainment Software Association (*ESA Class 19 Comments*) at 1, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%2019/Entertainment_Software_Association_Class19_1201_2014.pdf.

²²² *Id.* at 2.

instructions on how to circumvent access controls and install pirated games. The Joint Creators and Copyright Owners endorse ESA's arguments and also oppose this exemption 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, and that have flourished partly as a result of the protection that technologies protection measures provide."²²³

Based on the available record, NTIA cannot recommend a broad exemption for circumvention of access controls in gaming consoles for software interoperability at this time. The proponents provide general arguments that lack specificity. In fact, the current record to support this exemption is significantly less robust and detailed than it was in the last rulemaking.²²⁴

Hardware Repair

On the other hand, NTIA is persuaded that proponents have demonstrated that access controls in video game consoles inhibit users' ability to repair console hardware.²²⁵ The record indicates that circumvention is sometimes necessary to effectively perform these repairs, and NTIA is persuaded that these repairs will neither adversely affect the market value of copyrighted works nor promote infringing activity.²²⁶ Console owners may need to perform repairs well after warranty coverage has expired and, without this exemption, owners of consoles are adversely affected.²²⁷ The alternatives to circumvention offered by opponents do not, in many cases, obviate the need for an exemption to allow owners to repair their consoles. Most of

²²³ See Class 19 Comments of the Joint Creators and Copyright Owners (*Joint Creators Class 19 Comments*) at 2, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%2019/Joint_Creators_and_Copyright_Owners_Class19_1201_2014.pdf.

²²⁴ There was a dearth of evidence supporting the initial petition related to third-party software. By contrast, the exemption proposed during the last rulemaking was far more robust and contained better specificity of the intended use for the exemption. See, e.g., Class 3 Comments of the Electronic Frontier Foundation at 19-20, Docket No. RM 2011-07, available at <http://www.copyright.gov/1201/2011/initial/eff.pdf>.

²²⁵ NTIA recognizes that the act of repairing a console may involve the replacement of malfunctioning hardware components, and intends to include component replacement within the scope of this proposed exemption.

²²⁶ See Class 19 Response to Post-Hearing Questions of iFixit at 1 (*iFixit Class 9 Response to Post-Hearing Questions*), available at http://copyright.gov/1201/2015/post-hearing/answers/Class_19_Hearing_Response_iFixit_Docket_No_2014-07_2015.pdf (noting that "[i]t is necessary to circumvent technological protection measures in order to replace the optical drive in a Sony Playstation 3 or a Microsoft Xbox 360" and providing specific instructions on doing so). NTIA concluded in the last rulemaking that an exemption "limited to unauthorized repairs would not undermine console manufacturers' existing business models or hinder innovation in the video game industry." See *NTIA 2012 Letter* at 7. To be clear, NTIA notes that the term "repair" for purposes of this exemption should also include the circumstances when replacing malfunctioning hardware will repair the console that is not functioning. This includes replacing the hardware with refurbished hardware when necessary.

²²⁷ See *May 20 Transcript Hearing* at 280-307 (providing a lengthy discussion on how repairs are performed, how owners currently repair their consoles, and the various obstacles that are present when performing such repairs).

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.²²⁸ NTIA commends manufacturers for providing such repair options; however, NTIA does not believe that this should be the only mechanism through which owners can have their gaming consoles repaired. In addition, an exemption would be needed for owners of consoles that are no longer supported by the manufacturer.

Therefore, NTIA recommends an exemption to allow circumvention of access controls in gaming consoles to repair defective console hardware, and again suggests the following language similar to the 2012 proceeding:

Computer programs that enable video game console hardware to operate with the console operating system, when circumvention is initiated by the owner of the console for the purpose of repairing malfunctioning hardware, for systems that are obsolete or no longer covered by manufacturer warranty.

3. Smart Televisions (Class 20)

Proponents seek the ability to circumvent access controls in smart televisions (TVs) to allow the installation of user-supplied software.²²⁹ Proponents claim that this exemption would fall within fair use and would also make smart TVs more useful and accessible.²³⁰

Although this is the first time that an exemption for smart TVs has been requested, NTIA notes that in many ways this class is similar to the circumvention of access controls in mobile devices for software interoperability. The record indicates that some manufacturers restrict access to TV operating systems through TPMs that prevent the installation of third-party applications.²³¹ Proponents would like to enable their smart TVs to execute third-party

²²⁸ See *iFixit Class 9 Response to Post-Hearing Questions* at 2-3 (explaining the various repair services offered by manufacturers including costs and common complaints).

²²⁹ See Initial Petition of the Software Freedom Conservancy (*Software Freedom Conservancy Petition*), Docket No. 2014-07, available at http://copyright.gov/1201/2014/petitions/Software_Freedom_Conservancy_1201_Initial_Submission_2014.pdf. One of the types of applications proponents seek to install are “FLOSS applications” that are “licensed according to terms that permit and encourage users to copy, modify, and share them freely.” Class 20 Comments of Software Freedom Conservancy (*Software Freedom Conservancy Class 20 Comments*) at 4, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_SFC_Class20.pdf.

²³⁰ See *Software Freedom Conservancy Petition* at 2-3.

²³¹ See Class 20 Comments of the Joint Creators and Copyright Owners (*Joint Creators Class 20 Comments*) at 2, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%2020/Joint_Creators_and_Copyright_Owners_Class20_1201_2014.pdf; Class 20 Comments of LG Electronics U.S.A., Inc. at 2, Docket No. 2014-07, available at http://copyright.gov/1201/2015/reply-comments-050115/class%2020/ReplyComments_LongForm_LG_Class20.pdf (acknowledging that manufacturers are installing TPMs on their smart TVs).

applications, similar to mobile devices owners. In addition, proponents claim 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.²³²

The Joint Creators and Copyright Owners oppose this exemption and claim that circumvention of access controls on smart TVs would increase piracy of applications designed for use on smart TVs, and that circumvention would also be detrimental to the secure and trustworthy innovative platforms that consumers demand.²³³ These are important concerns, but are not sufficient to obviate the need for an exemption when balanced against the harms demonstrated by the proponents. Furthermore, there is no evidence that smart TV manufacturers depend or rely on smart TV software to recoup development costs, or that widespread circulation of software unapproved by the smart TV manufacturer would negatively affect the market for software that runs on smart TVs.²³⁴

Circumvention to achieve software interoperability in smart TVs does not raise significantly different issues than those the Register has previously considered regarding the jailbreaking of mobile phones. Specifically, the Register has repeatedly found that “making minor alterations in the firmware of an iPhone (or any smartphone) in order to permit independently created software applications to run on the [smartphone] is a fair use.”²³⁵ The Register concluded in 2010 that when jailbreaking to make the operating system on that device interoperable with an independently created application, any modifications made purely for the purpose of such interoperability are noninfringing fair uses.²³⁶

²³² See *Software Freedom Conservancy Class 20 Comments* at 5 (cataloging user-developed software modifications that allow smart TV owners to “modify subtitles to be larger, brighter, or outlined to enhance readability” and “change the aspect ratio, resolution, or scale of the TV’s display,” among other actions).

²³³ See *Joint Creators Class 20 Comments* at 4-5 (describing the benefits of providing “software developers and consumers with reliable ecosystems within which to offer innovative new products” and also describing apps that enable piracy such as Popcorn Time).

²³⁴ See *Class 20 Reply Comments of Software Freedom Conservancy* at 5, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/reply-comments-050115/class%2020/ReplyComments_LongForm_SFC_Class20.pdf (“Prior unlocking exemptions demonstrate why Opponents’ concern of negative market effects is unrealistic. The exemptions granted for smartphone and tablet unlocking have increased, not harmed, both software availability and innovative uses of the devices.... A similar effect can be expected if this exemption is granted. Making access easier for developers, researchers, and technically inclined end-users will promote software availability and innovation.” (Citation omitted.)).

²³⁵ *2012 Register of Copyrights Recommendation* at 72 (brackets in original) (citing *2010 Register of Copyrights Recommendation* at 92-93).

²³⁶ See *2010 Final Rule* at 43,830 (“On balance, the Register concludes that when one jailbreaks a smartphone in order to make the operating system on that phone interoperable with an independently created application that has not been approved by the maker of the smartphone or the maker of its operating system, the modifications that are made purely for the purposes of such interoperability are fair uses. Case law and Congressional enactments reflect a judgment that interoperability is favored. The Register also finds that designating a class of works that would permit jailbreaking for purposes of interoperability will not adversely affect the market for or value of the copyrighted works to the copyright owner.”).

Opponents call on the Register to reevaluate this analysis in light of the *Oracle America, Inc. v. Google Inc.* case.²³⁷ In that case, Google copied names and interface specifications (collectively, a description of the ways in which software developers can invoke these built-in programs, known as application programming interfaces or APIs) from 37 sets of programs in the Java platform’s standard library while creating the Android operating system. The Federal Circuit rejected Google’s claims that the APIs constituted methods of operation and were therefore ineligible for copyright protection. The Joint Creators and Copyright Owners claim that this case calls into question the Register’s analysis from prior rulemakings because

[t]hat reasoning deprives software of its rightful status as a fully protectable category of copyrightable works merely because it has some functional elements. *By concluding that every copy of a software program, no matter how trivial the differences between the original and the reproduction, qualifies as a fair use simply because it enables interoperability, the Register effectively, if perhaps unintentionally, recognized the “‘interoperability exception’ to copyrightability”* that the Federal Circuit rejected in the Oracle case.²³⁸ (*Emphasis added.*)

Opponents’ argument appears to conflate copyrightability and fair use, which are two different and distinct issues. NTIA has not found an instance in which a governmental entity or a participant in this proceeding has suggested that a particular class of works for which a jailbreaking exemption has been sought is not copyrightable merely because copying or modification of certain elements may be necessary for interoperability purposes.²³⁹ If this were the case, then a discussion about fair use or any section of Title 17 would not be necessary because non-copyrighted works do not fall within the purview of the Copyright Act.²⁴⁰ To the contrary, NTIA, the Register, and the Librarian have acknowledged and consistently recognized that the software and firmware installed in electronic devices are generally copyrighted works, which are subject to all the protections and limitations that the Copyright Act provides.²⁴¹ NTIA could not find an instance where the Register has recognized the concept of an “interoperability exception to copyrightability” as the opponents claim. Therefore, NTIA believes that this

²³⁷ See *Joint Creators Class 20 Comments* at 3 (citing *Oracle Am., Inc. v. Google Inc.*, 750 F.3d 1339 (Fed. Cir. 2014), *cert. denied*, 135 S. Ct. 2887)).

²³⁸ *Id.* at 3-4.

²³⁹ NTIA notes that, in 2012, the Librarian opined that “one engaged in jailbreaking need only modify the functional aspects of the firmware, which may or may not be subject to copyright protection.” *2012 Final Rule* at 65,264. However, this statement, in and of itself, is not a determinative conclusion that the firmware is *not* copyrightable.

²⁴⁰ See *2012 Final Rule* at 65,271 (“The prohibition on circumvention of technological protection measures thus does not apply to public domain materials because such materials are not protected under Title 17.”); see also *2012 Register of Copyrights Recommendation* at 13-15 (further discussing the inapplicability of Section 1201 of the DMCA to non-copyrighted works).

²⁴¹ In 2010 and in 2012, proposed exemptions for software and network interoperability purposes were evaluated under the under Fair Use (17 U.S.C. § 107) and Essential Step (17 U.S.C. § 117(a)) tests. See *2010 Final Rule* at 43,828-32; *2012 Final Rule* at 65,263-66; *2012 NTIA Letter* at 10-14.

argument is without merit, and that the *Oracle America, Inc. v. Google Inc.* case—which hinges on the distinction between a computer program and its method of operation, rather than the copyrightability of the program itself—is inapposite to this proceeding.

Having analyzed the record, NTIA believes that designating a class of works that would allow circumvention of access controls in smart TVs will not adversely affect the market value of copyrighted works, and will provide relief from the harm proponents demonstrated. Accordingly, NTIA recommends the following exemption:

Computer programs that enable televisions to execute lawfully obtained software, where circumvention is accomplished for the sole purposes of enabling interoperability of such software with programs on the television, or removing software from the television.²⁴²

E. Data Access, and Diagnosis, Repair, or Modification of Software-Driven Devices

1. Motorized Land Vehicles (Class 21)

Proponents seek to circumvent TPMs restricting access to computer programs within the electronic control units (ECUs) that control the functioning of motorized land vehicles, including personal automobiles, commercial motor vehicles, and agricultural machinery, for purposes of lawful diagnosis and repair, or aftermarket personalization, modification, or other improvements.²⁴³ Under the exemption as proposed, circumvention would be allowed when undertaken by or on behalf of the lawful owner of the vehicle. The law and record support an exemption for lawful diagnosis, repair, or modification of motor vehicles and agricultural machinery.²⁴⁴

Proponents seek to circumvent access controls protecting vehicle software for purposes that include, but are not limited to, improving fuel economy, traditional engine tinkering, and

²⁴² NTIA proposes an exemption that is consistent with the exemption for software interoperability of mobile devices.

²⁴³ The TPMs at issue that prevent access to the vehicle's ECU include: proprietary software that must be combined with a compatible cable, computer memory modifications, and encryption. *See* Class 21 Comments of the University of Southern California Intellectual Property Law Clinic (*USC Clinic Class 21 Comments*) at 5-6, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments020615/InitialComments_longform_USC_Class21.pdf; *See* Class 21 Comments of the Electronic Frontier Foundation (*EFF Class 21 Comments*) at 4-5, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_longform_EFF_Class21.pdf.

²⁴⁴ For the purposes of this exemption, we rely on the definition of “motor vehicles” found in 49 U.S.C. § 13102. Agricultural machinery is left intentionally broad, to ensure that all devices identified by proponents are included, recognizing that the definition of such class of machines varies.

modifying and repairing vehicles.²⁴⁵ The proponents argue that, without an exemption, manufacturers are afforded extended, long-term control over vehicles via the TPMs on the ECUs.²⁴⁶

Proponents state that modifications allow vehicles and agricultural machines to be more accessible, adaptable, and appropriate to particular user needs, and that owners, and especially farmers, do not expect this practice of tinkering with a product they own to be illegal.²⁴⁷ Meanwhile, opponents cite industry practices and third party repair tools provided by manufacturers as alternatives to circumvention.²⁴⁸

However, proponents cite problems relating to the delay associated with waiting for dealer-certified mechanics to make necessary repairs, putting farmers at the “mercy of their equipment dealer’s time schedule,” which can interfere with the harvest schedule.²⁴⁹ According to one

²⁴⁵ See *EFF Class 21 Comments* at 6-7 (“In order to facilitate diagnosis and repair, users must sometimes modify vehicle software. One common example of this arises when a user is trying to understand what part of a complex system – their vehicle – is causing a particular malfunction. In order to narrow down the possibilities, it is common to disable certain hardware components, such as sensors or fans. Disabling these components requires access to and modification of vehicle firmware.”); *USC Clinic Class 21 Comments* at 10 (“Repairing agricultural machinery to restore it to its original specifications, may, in some instances, require copying the vehicle software.... Often, farmers putting on different size tires, wider axels, longer-reach arms, etc., may need to modify the embedded software for a particular machine to function properly. Additionally, farmers often must modify their equipment to comply with new legal regulations, such as adding the capability to track certain types of data for regulatory agencies. Such modifications often require retrofitting new devices into older machines, which requires accessing the ECU to install.”).

²⁴⁶ See *EFF Class 21 Comments* at 19 (citing examples of a “starter interrupter” that can shut down a purchaser’s car if they are late on loan payments or drive outside a designated area, and French automobile company Renault’s practice of offering an electric car with a “rented” battery capable of being shut off remotely); *id.* at 7 (“Without the ability to manipulate software in the course of diagnosis and repair, users are often forced to wait for technicians with proprietary systems to become available or replace parts that may or may not be faulty, creating waste and unnecessary expense.”).

²⁴⁷ See *Class 21 Comments of Farm Hack*, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_FarmHack_class21.pdf.

²⁴⁸ See *GM Class 21 Comments* at 7 (“GM and other OEMs, provide access to their diagnostic and technical information in order to facilitate repair through subscription services, which do not require circumvention of TPMs.”); *Class 21 Comments of John Deere (John Deere Class 21 Comments)* at 11, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%2021/John_Deere_Class21_1201_2014.pdf (describing the JDLink and Service Advisor tool for John Deere vehicles that provide diagnostics and gives diagnostic trouble codes to update software without the need for circumvention); *Class 21 Comments of Auto Alliance (Auto Alliance Class 21 Comments)*, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments032715/class%2021/Auto_Alliance_Class24_1201_2014.pdf (demonstrating how manufacturers are providing third party repairers the tools they need).

²⁴⁹ *USC Clinic Class 21 Comments* at 4; see also *Class 21 Reply Comment of David Ricotta*, Docket No. 2014-07, available at http://copyright.gov/1201/2015/reply-comments-050115/class%2021/ReplyComments_ShortForm_Ricotta_Class21.pdf (“This exemption will allow for customers to make field repairs when their cars break. Not all drivers of a particular make or model has access to a manufacturer-affiliated dealer/repair shop for their specific car within a reasonable distance, or can afford a day off work to get their car seen by a manufacturer-affiliated dealer/repair shop.”); see *Class 21 Comments of iFixit (iFixit*

proponent, the problems arising from the inability to modify and customize tractors is causing price and demand for old tractors to increase, while demand for newer tractors decreases.²⁵⁰ An exemption would enable the longstanding practices that auto enthusiasts and mechanics engage in to modify their vehicles to continue.²⁵¹

NTIA finds that proponents have shown that the intended use of computer programs embedded in vehicles is likely to be noninfringing under fair use principles²⁵² as well as Section 117.²⁵³ Proponents assert, and NTIA agrees, that fair use allows for “tinkering” and modification of vehicle software.²⁵⁴ In a fair use test under the statute, the first factor weighs in favor of fair use because it involves a variety of transformative purposes.²⁵⁵ The second factor also suggests fair use because the vehicle firmware contains unprotected elements that cannot be examined without copying, justifying reverse engineering.²⁵⁶ The third factor is satisfied because while the users are accessing and copying the entire ECU’s firmware, this action is necessary to understand the functionality of the vehicle.²⁵⁷ The fourth factor weighs in favor of fair use because there is no evidence of harm to the market for the copyrighted firmware. Proponents are not making copies of the computer program for purposes of distribution, nor do opponents show that there is likely to be an impact on the market for the software that operates the vehicle, independent of the vehicle itself.

The question of ownership is an important one here and was highly debated on the record. For example, Section 117 permits the copying or adaptation of a computer program by the owner of a copy of the computer program as an “essential step” in the utilization of the program, and by

Class 21 Comments) at 3, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComment_shortform_KWiens_Class21.pdf. (“When the equipment breaks or needs maintenance, farmers are dependent on dealers and manufacturer technicians – a hard pill to swallow for farmers, who have been maintaining their own equipment since the plow.”).

²⁵⁰ See *iFixit Class 21 Comments* at 3.

²⁵¹ See *EFF Class 21 Comments* at Appendix A (statements of car enthusiasts submitted as evidence including a statement by David Blundell describing his modifications to ECUs by reverse engineering and reprogramming a factory engine computer); *USC Clinic Class 21 Comments* at Exhibits 1-6 (recordings of video interviews of agricultural and mechanical workers in support of exemption).

²⁵² 17 U.S.C. § 107 (2012).

²⁵³ 17 U.S.C. § 117 (2012).

²⁵⁴ Opponents assert that modification is not fair use because it is not transformative and it would disrupt the existing market for diagnosing and repairing auto software. See, e.g., *GM Class 21 Comments* at 14-18.

²⁵⁵ See *USC Class 21 Comments* at 8 (“Users are literally adding new functions or modifying existing functions to suit different needs. In the case of all three categories of tinkering (diagnosis, repair, and modification), users are seeking to understand the functional aspects of the copyrighted work.”).

²⁵⁶ *Id.* at 9.

²⁵⁷ *Id.* at 10.

the owner or lessee of a machine for maintenance or repair purposes.²⁵⁸ Furthermore, with respect to farmers, proponents argue the law permits a farmer to modify embedded software for the purpose of improving efficiency and/or functionality as an essential step in utilizing it in conjunction with the farmer's machinery.²⁵⁹ Proponents assert that under *Krause v. Titleserv, Inc.* and *Vernor v. Autodesk, Inc.*, owners of a vehicle should be considered the owners of the copy of the underlying software for purposes of § 117.²⁶⁰ Opponents argue that there is no evidence that the owners of vehicles are the owners of a copy of the included software and that, consequently, § 117(a)(1) and § 117(a)(2) are not applicable.²⁶¹

However, the Electronic Frontier Foundation argues an examination of the “totality of the circumstances” suggests the transfer of ECU firmware is generally analogous to a sale of goods rather than a license.²⁶² NTIA is inclined to agree that, for the purposes of this exemption, the owner of a motor vehicle or agricultural equipment should be considered the owner of a copy of any software contained within the machine.²⁶³ It is not only essential as a policy matter that lawful purchasers of

²⁵⁸ 17 U.S.C. § 117 (a), (c) (2012).

²⁵⁹ See *USC Class 21 Comments* at 10-12 (citing *Krause v. Titleserv, Inc.*, 402 F.3d 119, 126 (2d Cir. 2005) (“finding that a business’ ‘additional of new features’ in computer software it lawfully owned a copy of qualified as exempt under 17 U.S.C. § 117(a)(1)) and *Storage Tech. Corp. v. Customer Hardware Engineering & Consulting, Inc.*, 421 F.3d 1307, 1314-5 (Fed. Cir. 2005) (“a company’s circumvention of a manufacturer’s password-encrypted system for the purposes of performing maintenance and repairs fell within the section 117 safe harbor and did not violate the DMCA”)).

²⁶⁰ The Second Circuit’s holding in *Krause* lays out an ownership test for the purposes of Section 117. Even without a formal title, a party who exercises “sufficient incidents of ownership” over the copy of the program is considered an owner for purposes of Section 117. See *Krause*, 402 F.3d at 124. In *Vernor*, the Ninth Circuit held that “when an individual receives a copy of a copyrighted work pursuant to a written agreement, ownership is determined by considering both formal and informal factors, such as whether the agreement was formally labeled a license; whether the copyright owner retained title to the copy; whether the copyright owner required the copy’s return or destruction; whether the copyright owner forbade duplication of the copy; and whether the copyright owner required the transferee to maintain possession of the copy throughout the duration of the agreement.” *EFF Class 21 Comments* at 12 (citing *Vernor v. Autodesk, Inc.*, 621 F.3d 1102, 1108 (9th Cir. 2010)).

²⁶¹ See, e.g., *Auto Alliance Class 21 Comments* at 4-6; *GM Class 21 Comments* at 10-12.

²⁶² See *EFF Class 21 Comments* at 14-15.

²⁶³ NTIA is further convinced by the many reply comments submitted on the record refuting opponents’ arguments regarding ownership. See, e.g., Class 21 Reply Comments of the Auto Care Association and the Automotive Parts Remanufacturers Association at 6-7, Docket No. 201407, available at http://copyright.gov/1201/2015/reply-comments-050115/class%2021/ReplyComments_ShortForm_ACA_APRA_Class21.pdf (“Consumers own their cars, including the copy of vehicle operation software embedded in the car’s [ECU], and have a right of privacy to control distribution of their personal data over telematics software. Auto Car and APRA reject any suggestion by the manufacturers and manufacturer associations that consumers do not own every part of the vehicle they purchase, including the copy of the software that regulates vehicle operation and the information generated by the use of the vehicle[.]”); Class 21 Reply Comments of iFixit, Docket No. 2014-07, available at http://copyright.gov/1201/2015/replycomments050115/class%2021/ReplyComments_ShortForm_Ifixit_Class21.pdf (“[Opponents] are trying to eviscerate the notion of ownership. Sure, we pay money for their vehicles. But we don’t really own them anymore.”); Class 21 Reply Comments of the USC Clinic at 4, Docket No. 2014-07, available at http://copyright.gov/1201/2015/replycomments050115/class%2021/ReplyComments_LongForm_USCIP_Class21.p

motor vehicles are not deprived of traditional notions of ownership as vehicles become increasingly equipped with software (at the very least, for purposes of this rulemaking process),²⁶⁴ but it is also consistent with prior exemptions regarding ownership of software within devices.²⁶⁵

GM, John Deere, and the Auto Alliance oppose this exemption.²⁶⁶ Opponents make a cursory attempt to show that circumvention of TPMs would lead to distribution of pirated copies of the software within the ECU. They also assert that, by gaining access to the firmware, individuals may also gain access to copyrighted works such as music and audiovisual works in vehicle entertainment systems.²⁶⁷ On the latter point, NTIA agrees that copying any of the audiovisual and musical works cited would likely constitute infringement and are outside the scope of the proposed exemption. However, proponents for this class have not contemplated any activities that would involve such works.

Parties opposing this exemption primarily address concerns unrelated to copyright infringement, including vehicle safety, increased liability, and emissions standards. Opponents argue that proponents do not show they have the requisite skill to ensure the desired

df (“No respondent - including John Deere – introduced any evidence to support their claims that they placed restrictions on owners of agricultural machines or that they wished any such restriction to be a ‘contractual matter.’ Thus, the evidence compels a finding that, at least in the context of agricultural machinery, such a copy is sold to the purchaser of the machine along with the machine itself.”); Class 21 Reply Comments of the National Corn Growers Association, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/reply-comments-050115/class%2021/ReplyComments_ShortForm_NCGA_Class21.pdf (“Recently, troublesome comments were made on Proposed Class 21 that muddy the definition of ownership and blur the lines between software, hardware, and the ability to diagnose, repair, personalize, modify, or improve lawfully owned farm equipment and the computer programs that help operate them.... The recent comments surrounding copyright activities as it pertains to legally owned farm machinery is not well understood among farms, but there is reason to be concerned as clear definitions of ownership are potentially being misconstrued.”)

²⁶⁴ See Class 21 Reply Comments of the American Automobile Association, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/replycomments050115/class%2021/ReplyComments_ShortForm_AAA_Class21.pdf (“Suggesting that a vehicle owner, or a consumer-approved third-party, repairing or augmenting a personal motor vehicle is a copyright violator under the Digital Millennium Copyright Act is draconian and would deeply undercut consumer rights, choice and widespread public notions about the ownership of vehicles and the data they generate.”).

²⁶⁵ The Register concluded in 2012 that the state of the law with regard to software ownership remained “indeterminate,” rejecting opponents’ claims that owners of a cell phone merely licensed the software and were not entitled to protection of § 117, and then stated that the ownership question was a “closer call.” See *2012 Final Rule* at 65,265.

²⁶⁶ See Class 21 Comments of the Association of Equipment Manufacturers (*Equipment Manufacturers Class 21 Comments*) at 1, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-032715/class%2021/Association_of_Equipment_Manufacturers_Class21_1201_2014.pdf (supporting John Deere’s comments); see also *GM Class 21 Comments* at 2 (noting that many safety regulations are federally mandated).

²⁶⁷ *John Deere Class 21 Comments* at 2 (“TPMs for vehicle software for entertainment systems protect copyright owners of copyrighted content against the unauthorized reproduction and distribution of copyrighted works. For example, vehicle software for entertainment systems supports the playing of copyrighted music files and copyrighted audio books, among other expressive works.”).

modifications comply with vehicle safety standards or environmental regulations.²⁶⁸ Auto Alliance lists several examples of potential dangers associated with vehicle system modifications, 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.²⁶⁹ Opponents also claim that the exemption would have an adverse effect on risk assessment for product liability and insurance.²⁷⁰

Opponents also express concerns that modifications and repairs could cause vehicles to fall out of regulatory compliance with emission standards, a fear that is shared by some regulatory bodies.²⁷¹ NTIA appreciates these concerns, and indeed believes that the appropriate regulatory authorities will continue to ensure compliance with federal and state laws that control safety features and emission. NTIA notes, however, that granting an exemption from the prohibition against circumvention does not authorize a vehicle owner to violate any federal, state, or local laws.²⁷² Furthermore, it is unclear whether the act of circumvention is necessarily prohibited by other statutes.²⁷³ Anyone engaging in circumvention under this proposed exemption must still comply with applicable laws and regulations, both state and federal.²⁷⁴ The relevant regulatory bodies would retain authority to enforce any applicable law or regulation. Therefore, the

²⁶⁸ *Equipment Manufacturers Class 21 Comments* at 1.

²⁶⁹ *See Auto Alliance Class 21 Comments* at 17-19.

²⁷⁰ Class 21 Comments of the Association of Global Automakers at 8, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-032715/class%2021/Association_of_Global_Automakers_Class21_1201_2014.pdf.

²⁷¹ *See generally* Letter from Geoff Cooper, Assistant General Counsel, Environmental Protection Agency, to Jacqueline C. Charlesworth, General Counsel and Associate Register of Copyrights (*EPA Letter*) (July 17, 2015), *available at* http://copyright.gov/1201/2015/USCO-letters/EPA_Letter_to_USCO_re_1201.pdf.

²⁷² For example, it is a violation of federal law under Section 203(a)(3) of the Clean Air Act “for any person to remove or render inoperative any device or element of design installed on or in a motor vehicle or motor vehicle engine in compliance with regulations under this subchapter” or to “manufacture or sell, or offer to sell, or install, any part or component intended for use with, or as part of, any motor vehicle or motor vehicle engine, where a principal effect of the part or component is to bypass, defeat, or render inoperative any device or element of design installed on or in a motor vehicle or motor vehicle engine in compliance with regulations under this subchapter.” 42 U.S.C. § 7522(a)(3) (2012).

²⁷³ The Clean Air Act and applicable EPA regulations do not contemplate whether the breaking of a TPM on its own constitutes a violation of the Act or applicable regulation. Nor does the EPA argue that this is the case in its letter. Instead, the EPA is concerned with the subsequent action taken after the act of circumvention. *See EPA Letter* at 2-3. NTIA reiterates that any repairs or modification must be in compliance with and adhere to applicable laws and regulations regarding emissions.

²⁷⁴ *See USC Clinic Class 21 Comments* at 15 (“The only concrete examples of the potential for dangerous or harmful modifications that Respondents have provided are modifications that are already illegal for reasons unrelated to copyright law. As Respondents themselves note, tampering with vehicle odometers violates “the laws of virtually every state;” the unsafe placement of entertainment systems violates “federal motor carrier safety regulations;” and aftermarket tampering with emissions controls violates existing EPA regulations. Granting the exemption would not lift the bans on those types of modifications. They will remain illegal.”).

Copyright Office should, as previously mentioned, focus on questions relevant to copyright law rather than on unrelated matters, important as those issues may be.

NTIA is sympathetic to opponents' concerns, but is not convinced that opponents have proven the requisite harm to their copyright interests to warrant denial of an exemption. That said, given the various non-copyright concerns raised with regard to this class, NTIA proposes including a provision in the exemption explicitly stating that it does not preclude liability under other applicable laws. NTIA also recognizes that granting this exemption would not preclude the use of contractual agreements (such as warranties) by manufacturers as a means to reduce liability risks.

Contrary to opponents' concerns, proponents have argued that enabling owners to modify and repair their vehicles could actually help to eliminate safety dangers, and could potentially reduce emissions beyond current standards.²⁷⁵ Further, to the extent that security risks increase as bad actors, acting outside the permission of this exemption, become more sophisticated in accessing the ECUs in vehicles, NTIA urges that appropriate measures be taken by the relevant regulatory agencies. Opponents request that the Librarian "show regulatory deference to the other federal government agencies" by denying this proposed exemption.²⁷⁶ Yet in basing a denial of an exemption on reasons largely unrelated to copyright law, the Librarian would, in effect, be claiming expertise and authority in policy areas far beyond the Librarian's focus, which are best left to the relevant regulatory bodies. Because manufacturers seem to be installing the TPMs at issue here for largely non-copyright purposes, granting an exemption for this class would be the appropriate course of action. Accordingly, NTIA suggests the following exemption:

Computer programs embedded in motorized land vehicles or agricultural machinery, when circumvention is initiated by or at the request of the owner of the vehicle or machinery, in order to make repairs or modifications to the vehicle or machinery. This exemption does not obviate the need to comply with other applicable laws and regulations, such as those relating to vehicle safety or environmental protection.

²⁷⁵ Proponents cite many examples of inventions and safety improvements that "originated in the hobbyist community independent of the automakers." See Class 21 Reply Comments of the Specialty Equipment Market Association, Docket No. 2014-07, available at http://copyright.gov/1201/2015/reply-comments-050115/class%2021/ReplyComments_LongForm_SEMA_Class21.pdf. They include the following examples: cruise control to improve jerky car rides invented by engineer Ralph Teetor, Neurologist Dr. C. Hunter Sheldon's idea for the retractable seat belt, recessed steering wheels, reinforced roofs, roll bars, door locks, and passive restraints such as the air bag, "tinkerer" Robert William Kearns's invention of the first intermittent windshield wiper mechanism created by using off the shelf electronics, and hands-free technology such as Bluetooth hands-free technology, were all developed in the aftermarket. *Id.* Further, they assert that "so-called tinkerers" have also worked to improve emissions and fuel economy on vehicles. *Id.* at 3.

²⁷⁶ Class 22 Comments of John Deere (*John Deere Class 22 Comments*) at 4, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%2022/John_Deere_Class22_1201_2014.pdf.

2. Medical Devices (Part of Class 27)

Proponents seek the ability to “access the computer code and data outputs of medical devices,” and use this information to perform security and safety research, as well as to enable patients to make improved use of their health data.²⁷⁷ However, in light of the separate proposal to enable security research into computer programs generally (Class 25), it is more appropriate to cover the safety and security research aspect of proponents’ request in Class 25, and for the patient data access aspect to compose the entirety of this class (Class 27). This appropriately separates two distinct issues, and allows NTIA, the Copyright Office, and the Librarian to broadly consider security research rather than repeating its analysis across many separate classes.

With regard to patient data access, proponents seek an exemption to gather data from devices in real time for the purpose of monitoring device outputs such as heart rate, glucose levels, and other medical data.²⁷⁸ According to the Coalition for Medical Device Research (CMDR), an exemption is necessary because TPMs prevent access to patient data. Furthermore, these access controls are likely to become more prevalent in the near future because the FDA has recommended that manufacturers start employing technical measures to protect patient data on medical devices.²⁷⁹ The CMDR also claims the exemption is necessary because there is no alternative to circumventing TPMs to access the relevant information.²⁸⁰

Having analyzed the record, NTIA is persuaded that designating a class of works that would allow a patient and his or her doctor to have greater access to the patient’s medical data will not adversely affect the market value of the copyrighted software that runs the medical devices. There is no market for medical device software divorced from the device itself, nor is the software a replacement for the device, so this exemption would not harm the copyrighted software’s value.²⁸¹

NTIA is also persuaded that granting this exemption would provide relief from the harm that proponents have demonstrated. Proponents state they are harmed because they are unable to see and react to data collected by medical devices (*e.g.*, glucose spikes, heart rate drops) in real time.²⁸² NTIA agrees with proponents that making a patient wait for a medical appointment to

²⁷⁷ See Class 27 Comments of the Coalition for Medical Device Research (*CMDR Class 27 Comments*) at 2, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_longform_Coalition_of_Medical_Device_Researchers_Class27.pdf.

²⁷⁸ *Id.*

²⁷⁹ *Id.* at 9.

²⁸⁰ *Id.* at 24.

²⁸¹ *CMDR Class 27 Comments* at 14.

²⁸² See Transcript of May 29, 2015, Hearing on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Section 1201 – Digital Millennium Copyright Act (*May 29 Hearing Transcript*) at 8, Docket No. 2014-07, available at <http://copyright.gov/1201/2015/hearing-transcripts/1201-Rulemaking-Public-Roundtable-05-29-2015.pdf>.

access his or her own medical data is not a sufficient alternative to circumvention, because that is not a practical way to see medical data changes in real time.²⁸³ For example, if a patient receives a report at the doctor's office showing a glucose spike three weeks ago at a certain time, the patient will likely not remember what happened at that moment, and will be unable to take remedial action in order to prevent that kind of spike from repeating.²⁸⁴ When devices allow patients to monitor their data in real time, they may react in real time, which proponents believe could enable patients to improve their health.²⁸⁵

Opponents claim that acquiring these data will deteriorate a device's battery life faster than contemplated by the manufacturer, resulting in additional surgeries to replace the drained batteries.²⁸⁶ However, proponents assert 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.²⁸⁷ They further note that, for some devices such as insulin pumps, battery changing is a simple process involving no surgery at all.²⁸⁸ Granting an exemption aimed at increasing patient access to his or her own medical data would consequently provide relief from the harm that proponents have demonstrated and would not adversely affect the market for or value of the copyrighted software involved.²⁸⁹

At least one opponent, the Advanced Medical Technology Association, asserts that a medical device's output could be entitled to copyright protection based on its structure, format, and arrangement, and that the proponents' contemplated use of the output would not be a fair use of

²⁸³ See Class 27 Reply Comments of Public Knowledge (*PK Class 27 Reply Comments*) at 8, Docket No. 2014-07, available at http://copyright.gov/1201/2015/reply-comments-050115/class%2027/ReplyComments_LongForm_PublicKnowledge_Class27.pdf.

²⁸⁴ See *CMDR Class 27 Comments* at 24. As Public Knowledge pointed out in their comments, "Family members, guardians, and friends of patients also have cause to access the data, in order to provide care and support for loved ones. For example, a schoolchild with a glucose monitor could easily benefit from the school nurse, a parent, or a guardian having access to the data, so that those equipped with necessary medication in case of an emergency can react fastest." Class 27 Comments of Public Knowledge at 3, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_longform_PK_Class27.pdf.

²⁸⁵ See *May 29 Hearing Transcript* at 9-14 (Mr. West, a diabetic, discussing how the ability to monitor his glucose levels in real time allows him to quickly take action (*e.g.*, get glucose, take medicine) to avoid spikes or drops.).

²⁸⁶ See Class 27 Comments of LifeScience Alley at 4, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%2027/LifeScience_Alley_Class27_1201_2014.pdf.

²⁸⁷ See Class 27 Reply Comments of the Coalition for Medical Device Research (*CMDR Class 27 Reply Comments*) at 11, Docket No. 2014-07, available at http://copyright.gov/1201/2015/reply-comments-050115/class%2027/ReplyComments_LongForm_CMDR_Class27.pdf.

²⁸⁸ See *PK Class 27 Reply Comments* at 8. Footnote 12 provides an excellent example of the ease with which some devices' batteries can be changed. *Id.*

²⁸⁹ See 17 U.S.C. §1201(a)(1)(C)(iv) (2012).

the copyrighted material.²⁹⁰ However, NTIA is persuaded that the medical data collected from the device generally are not transferred as a direct copy of the manufacturer's database, nor is the new database identical to the manufacturer's in structure or format. Reportedly, when medical data are transmitted from the device, two things happen. First, the raw medical data are transferred to a wearable (such as a smart watch) or other device (such as a mobile phone) so that the patient may glance instantaneously at the output and react to it.²⁹¹ Second, the raw medical data are transferred to a new database, which is not copied from the manufacturer, to organize the data for future analysis.²⁹² The common element in structure and arrangement between the manufacturer's database and the new database appears to be the medical data themselves, which are likely to be construed as unprotectable facts.²⁹³ Copying such data likely would not constitute an infringing activity because the proponents would not replicate the manufacturer's potentially copyrightable database structure to arrange their medical information.

Moreover, in the event that collection of medical data from a device does involve copying a protectable database structure, that copying is likely to be a fair use. The uses contemplated by proponents are frequently noncommercial in nature, as they are focused on a patient obtaining his or her own medical data, and are often educational in character.²⁹⁴ Furthermore, the database being copied would likely be highly utilitarian in nature, and while a substantial portion of the database may be copied, "such taking is routinely appropriate given the nature of the use."²⁹⁵ It also is unlikely that copying a database containing personal medical data would have any effect on the market for that work, which is essentially nonexistent apart from the medical device on which it is contained.²⁹⁶

In conclusion, NTIA is convinced that this concern does not weigh against granting an exemption. Accordingly, NTIA suggests the following exemption:

²⁹⁰ See Class 27 Comments of the Advanced Medical Technology Association (*AdvaMed Class 27 Comments*) at 5, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%2027/AdvaMed_Class27_1201_2014.pdf.

²⁹¹ See *May 29 Hearing Transcript* at 20.

²⁹² See *id.* at 21-22.

²⁹³ See *id.* at 22. See also *Feist Publ'ns v. Rural Tel. Serv. Co., Inc.*, 499 U.S. 340, 350 (1991) (holding that facts—alone or in a compilation—are not original and thus not copyrightable).

²⁹⁴ See *CMDR Class 27 Comments* at 12.

²⁹⁵ *Id.*

²⁹⁶ *Id.*

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 performed by or at the direction of a patient seeking access to data generated by a device used by that patient. 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.

This exemption language is modeled from the language in the CMDR’s reply comments in this proceeding, but omits any security research related language, for the reasons discussed above.²⁹⁷ This configuration more precisely addresses opponents’ concerns that the proposed exemption was overly broad by adding the language “seeking access to information generated by his or her own device.”²⁹⁸ The revised exemption language also avoids any questions regarding ownership that may arise if medical device ownership schemes change. Opponents were concerned that the exemption was overly broad because it could include devices which do not output information.²⁹⁹ This language would eliminate that concern because the exemption does not include devices which do not generate information.

One other outstanding issue opponents raise in this proceeding is that medical devices are already regulated by the FDA, that they should remain under the FDA’s domain,³⁰⁰ and that granting this exemption would promote medical device misuse by patients.³⁰¹ NTIA recognizes that the FDA has considerable regulatory authority in the area of medical device safety;³⁰² however, the Copyright Office has the authority and expertise to address concerns about applicable *copyright* issues that arise in the context of medical devices. NTIA appreciates that parties have raised important questions about the safety and efficacy of medical devices, and NTIA is confident that the appropriate regulatory agencies will address any non-copyright issues that may arise once this exemption is granted. As NTIA’s proposed exemption language makes clear, “the circumvention exemption is not an exemption from other applicable regulations.”³⁰³

²⁹⁷ *CMDR Class 27 Reply Comments* at 23.

²⁹⁸ *AdvaMed Class 27 Comments* at 4.

²⁹⁹ *Id.* at 5.

³⁰⁰ *Id.* at 3.

³⁰¹ *Id.* at 4.

³⁰² Overview of Medical Devices and Their Regulatory Pathways, Food and Drug Administration, <http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHTransparency/ucm203018.htm>.

³⁰³ Letter from Bakul Patel, Associate Director for Digital Health, Center for Devices and Radiological Health, U.S. Food and Drug Administration, to Jacqueline C. Charlesworth, General Counsel and Associate Register of Copyrights, U.S. Copyright Office, at 5 (Aug. 18, 2015), available at http://copyright.gov/1201/2015/USCO-letters/FDA_Letter_to_USCO_re_1201.pdf.

Therefore, the Copyright Office should, as previously mentioned, focus on questions relevant to copyright law rather than on unrelated matters, important as those issues may be.

While concerns about medical device misuse are beyond the scope of copyright law, NTIA appreciates the serious underlying issues. That said, opponents do not present evidence to support their claim that an exemption will lead to misuse, and baldly assert that proponents' proposed use "is an unauthorized use of the device manufacturer's systems, which are meant for patient care."³⁰⁴ This seems to refer to the security research portion of the proposed exemption, not to patient data use, or it would imply that a patient's accessing his or her own data does not contribute to patient care. As proponents explained, the purpose of this exemption is to allow patients and doctors to more effectively use medical data and enhance treatment.³⁰⁵ Therefore, this issue does not weigh against granting an exemption.

Furthermore, if patients were to misuse their devices, the FDA already has a system in place to address the consequences of any potential misuse through their Mandatory Device Reporting regulation.³⁰⁶ Manufacturers, importers, and user facilities complete Mandatory Device Reports when there is a device-related death, serious injury, or malfunction, and as part of annual reports to the FDA.³⁰⁷ There are also labeling regulations³⁰⁸ in place so manufacturers can effectively inform patients and doctors of the warranties³⁰⁹ associated with medical devices. In addition, there are guidelines in place to design medical device interfaces to minimize patient misuse.³¹⁰ In summary, there are many mechanisms in place to address this particular concern. Apprehension over patient misuse is also another example of a non-copyright concern that has been raised in

³⁰⁴ *AdvaMed Class 27 Comments* at 4.

³⁰⁵ See Class 27 Comments of Jay Freeman, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_shortform_JFreeman_Class27.pdf, *CMDR Class 27 Comments* at 3.

³⁰⁶ See 21 C.F.R. § 803 *et. seq.* (2015).

³⁰⁷ Mandatory Reporting Requirements: Manufacturers, Importers and Device User Facilities, Food and Drug Administration (2015), available at <http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/PostmarketRequirements/ReportingAdverseEvents/ucm2005737.htm>. Patients, consumers, and health professionals may voluntarily report medical device adverse events or product problems to the FDA through MedWatch, the FDA's Safety Information and Adverse Event Reporting Program. Incidents are then available to the public online through the FDA's database, called the Manufacturer and User Facility Device Experience (MAUDE). See *Manufacturer and User Facility Device Experience Database - (MAUDE)*, Food and Drug Administration (2015) <http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/PostmarketRequirements/ReportingAdverseEvents/ucm127891.htm>.

³⁰⁸ See 21 C.F.R. § 801 *et seq.* (2015).

³⁰⁹ See *Guidance on Medical Device Patient Labeling*, Food and Drug Administration (2001) at 22, <http://www.fda.gov/RegulatoryInformation/Guidances/ucm070782.htm#additional>.

³¹⁰ See *Medical Device Use-Safety: Incorporating Human Factors Engineering into Risk Management*, Food and Drug Administration (2000) at 18, available at <http://www.fda.gov/downloads/MedicalDevices/.../ucm094461.pdf>.

this proceeding, and NTIA again emphasizes that it is a subject best addressed outside of a rulemaking conducted pursuant to copyright law.

F. Using Unsupported Software

1. Video Games (Class 23)

Proponents seek the ability to circumvent access controls to allow video game users to continue playing lawfully-obtained games once video game developers have discontinued official support.³¹¹ Proponents' requested exemption would allow for circumvention of TPMs on "consoles, personal computers or personal handheld gaming devices."³¹² Two separate but related groups would like to take advantage of this exemption: (1) video game players who would circumvent to re-enable functionality for private use, and (2) scholars and archivists who would circumvent to allow for the study, preservation, and museum exhibition of video games.³¹³ There is sufficient evidence in the record that the proposed uses of these two groups should both be included in the proposed exemption. Moreover, in some cases the two types of proposed uses are intertwined, as scholars and archivists often depend on the video game player community to engage in the reverse-engineering necessary to re-enable lost video game functionality.³¹⁴

Proponents argue compellingly that multiplayer gameplay in particular is a core functionality of many of the video games at issue, and that users expect this functionality when purchasing games, citing the opinions of professional video game reviewers and comments submitted by the

³¹¹ NTIA agrees with EFF that the proposed exemption should apply only to games where servers are used to connect multiple players and where "all or nearly all of the audiovisual content resides in the player's local copy of the game." It should not apply to "persistent world" games (e.g., World of Warcraft) that remain active and intact even when a player signs off; these games generally cannot be recreated after the developer's servers are shut down. See Class 23 Comments of the Electronic Frontier Foundation (*EFF Class 23 Comments*) at 2, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_longform_EFF_Class23.pdf. EFF added further detail to the definition for this proposed class during the Los Angeles hearing: "A game that would be covered by this proposed exemption is a game that can be restored using a lawfully-owned copy and analysis of server traffic but without a copy of the server software." *May 20 Hearing Transcript* at 228. Additionally, while this class and Class 19 – Interoperability of Third-Party Applications in Video Game Consoles, both address video games, NTIA does not believe that there is an overlap between the classes, because in this class there is no "malfunctioning" hardware or "obsolete" system involved. See *supra* Class 19 – Interoperability of Third-Party Applications in Video Game Consoles, page 46.

³¹² *EFF Class 23 Comments* at 1. NTIA understands the term "personal handheld gaming devices" to mean devices whose primary purpose is the playing of video games (e.g., Nintendo DS).

³¹³ See *id.* at 2 ("This exemption would serve player communities that wish to continue using their purchased games, as well as archivists, historians, and other academic researchers who preserve and study videogames and are currently inhibited by legal uncertainty because of §1201(a)(1).").

³¹⁴ See Reply Comments of the Electronic Frontier Foundation (*EFF Class 23 Reply Comments*) at 14, Docket No. 2014-07, available at http://copyright.gov/1201/2015/reply-comments-050115/class%2023/ReplyComments_LongForm_EFF_Class23.pdf.

player community in this proceeding.³¹⁵ Opponents argue that users do not consider multiplayer functionality a central feature that they are paying for when they purchase a video game.³¹⁶ This argument does not seem to reflect the reality of the video game market, and does not effectively rebut the evidence in the record.³¹⁷ Additionally, the record shows that the notice consumers may receive from the video game publisher regarding the discontinuation of multiplayer support is inconsistent at best.³¹⁸ Proponents even present examples of video games where a publisher discontinued multiplayer support without any prior public announcement.³¹⁹

The proposed use in this case is likely to qualify as a noninfringing fair use. Under the first statutory fair use factor, the purpose of the use in this case is personal and noncommercial. Opponents argue that, since the proposed use is not transformative, the first factor weighs against

³¹⁵ See *EFF Class 23 Reply Comments* at 6 (“Numerous game enthusiasts submitted comments to the Digital Right to Repair Coalition’s website regarding this exemption proposal, expressing their view that multiplayer play is “critical to the games that I play,” and that most games are “crippled without online play.” In particular, commenters identified the current games Star Wars: Battlefront, Titanfall, Destiny, Overwatch, Battlefield 2142, and Battlefield 3, and older games including Starcraft, Richard Burns Rally, Tribes 2, Grand Theft Auto V, and versions of Street Fighter as examples of games where multiplayer play is central.” (Citation omitted)).

³¹⁶ See Class 23 Comments of the Entertainment Software Association (*ESA Class 23 Comments*) at 8-9, Docket No. 2014-07, available at [http://copyright.gov/1201/2015/comments-032715/class%2023/Entertainment Software Association Class23 1201 2014.pdf](http://copyright.gov/1201/2015/comments-032715/class%2023/Entertainment%20Software%20Association%20Class23%201201%202014.pdf) (“[T]he access controls for multiplayer gameplay typically also restrict access to a wide range of other online network services including, for example, downloadable content, leaderboards, badges, chat, and other social features. Significantly, the user typically must register—and sometimes pay—for this suite of online network services separately; they almost never are included”); Class 23 Comments of the Joint Creators and Copyright Owners at 5, Docket No. 2014-07, available at [http://copyright.gov/1201/2015/comments-032715/class%2023/Joint Creators and Copyright Owners Class23 1201 2014.pdf](http://copyright.gov/1201/2015/comments-032715/class%2023/Joint%20Creators%20and%20Copyright%20Owners%20Class23%201201%202014.pdf) (affirming ESA’s arguments that server-supported multiplayer mode is not a core functionality of video games).

³¹⁷ See *EFF Class 23 Reply Comments* at 7-8 (presenting evidence that multiplayer mode is included in the purchase price of a game without payment of additional fees).

³¹⁸ Compare Class 23 Response to Post-Hearing Questions of the Entertainment Software Alliance (*ESA Class 23 Hearing Response*) at 3, Docket No. 2014-07, available at [http://copyright.gov/1201/2015/post-hearing/answers/Class 23 Hearing Response ESA Docket No 2014-07 2015.pdf](http://copyright.gov/1201/2015/post-hearing/answers/Class%2023%20Hearing%20Response%20ESA%20Docket%20No%202014-07%202015.pdf) (“The specific language varies depending on the publisher, platform, and context, but publishers are committed to ensuring that when a consumer is making a purchasing decision about a game, that consumer has clear and prominent notice that server support for a game may someday be discontinued.”) with Class 23 Response to Post-Hearing Questions of Parham Gholami at 3, Docket No. 2014-07, available at [http://copyright.gov/1201/2015/post-hearing/answers/Class 23 Hearing Response Gholami Docket No 2014-07 2015.pdf](http://copyright.gov/1201/2015/post-hearing/answers/Class%2023%20Hearing%20Response%20Gholami%20Docket%20No%202014-07%202015.pdf) (“Many older titles which featured online multiplayer functionality did not include any warning on the box or in the manual that online functionality would be removed. Electronic Arts is one of the only publishers to definitively state on the boxes of their titles, like *Madden NFL 2005*, that they could exercise the right to “retire” the game’s respective online features within thirty days’ notice. On the other hand, titles like *Amped 2* (2003), *MechAssault* (2002), *Halo 2*, *Animal Crossing: City Folk* (2008), *Super Smash Bros. Brawl* (2008), *Mario Kart Wii* (2008), and *SOCOM: U.S. Navy SEALs* (2002) made no such effort to make this clear to customers.”).

³¹⁹ See *EFF Class 23 Comments* at 3 (“Deactivation of servers on [centralized matchmaking server] platforms can spell the end of online play for many games at once. Gamespy, once a prolific operator of matchmaking servers, shut down a number of servers in 2012 without warning.”).

the proponents.³²⁰ However, proponents cite *Sony Corporation of America v. Universal City Studios* and the Register’s previous conclusions to support the contention that a personal, noncommercial 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.³²¹ Additionally, research and scholarship are favored uses under the fair use analysis.³²²

Regarding the nature of the copyrighted work under the second fair use factor, proponents persuasively argue that the proposed use would tend to involve modification of functional aspects of the software (including access controls themselves, among other elements), which are usually entitled to less copyright protection than a more expressive work would be.³²³ Opponents’ counterargument that the access controls “protect the interests of copyright law” does not seem to address the second factor directly.³²⁴

Regarding the amount and substantiality of the work taken under the third fair use factor, proponents argue that the portion of the game that needs to be modified to restore multiplayer

³²⁰ See *ESA Class 23 Comments* at 13-14 (citing *2012 Final Rule* at 65,274 (stating that “circumventing console code to play games and other entertainment content (even if lawfully acquired) is not a transformative use, as the circumvented code is serving the same fundamental purpose as the unbroken code.”)) .

³²¹ See *EFF Class 23 Reply Comments* at 10 (citing *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 449-50 (1984) (stating that time-shifting “merely enables a viewer to see such a work which he had been invited to witness in its entirety” and holding that such activity is fair use) and *2010 Register of Copyrights Recommendation* at 95 (“a use need not be transformative in order to be a fair use”)).

³²² 17 U.S.C. § 107 (2012). According to Henry Lowood, Curator for History of Science & Technology Collections and Film & Media Collections at the Stanford University Libraries, ‘Scholarship, teaching and research are concerned with the nature and histories of these virtual worlds as worlds, that is, as social communities with specific histories. They are also concerned with the structure of these worlds and the technical disciplines that create them, ranging from game design to computer programming. When access to a virtual world ceases with the ending of developer support, scholarly access to the historical world (events, activities, participants) represented by that game ends along with it. Moreover, researchers can no longer “get inside” the software, which inhibits efforts to understand the development of the technology. Critical historical research about game worlds is greatly handicapped when access to these worlds ends. The cost is not just lost game history, but lost cultural, technical and social history of the late-20th and early-21st centuries.’ *EFF Class 23 Comments* at Appendix, Statement of Henry Lowood, Stanford University. These uses are also favored by the DMCA itself, which states that “the Librarian shall examine... the impact that the prohibition on the circumvention of [TPMs] applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research.” 17 U.S.C. § 1201(C)(iii) (2012).

³²³ See *EFF Class 23 Comments* at 7 (“Modifying 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. Purely 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.”).

³²⁴ *ESA Class 23 Comments* at 14 (“The access controls at issue here protect the interests of copyright law by encouraging the creation and distribution of copyrighted works and by discouraging the distribution of pirated content. Specifically, the video game access controls decrease the unlawful distribution of infringing works and increase the legal supply of lawful copyrighted works.”).

functionality is a small portion of the overall software.³²⁵ Opponents state that the proposed use could involve “wholesale copying of the copyrighted work,” which should be disfavored.³²⁶ Proponents respond that even the creation of the copy of an entire program in order to circumvent is temporary and does not take more than is necessary for the users’ purpose.³²⁷ NTIA is convinced by proponents’ arguments regarding the second and third fair use factors.

With regard to the fourth factor, proponents argue that restoring functionality to a video game does not harm the market for that game, and may indeed increase its future value. Proponents further argue that discontinuation of multiplayer support for the games in question speaks to the diminishing market for works addressed by this exemption.³²⁸ Opponents’ statements that developers only choose to deactivate video game servers when player communities have effectively dried up seem to be contradicted by proponents’ evidence of deactivation for reasons unrelated to the number of continuing users.³²⁹ Opponents further argue that circumvention of video game access controls “would have the effect of diminishing the value of ... the affected code, because the compromised code could no longer serve as a secure method for the ... distribution of legitimate content.”³³⁰ Opponents also argue that the exemption could affect the market for video games generally, or lower developers’ profits on sequels or other subsequently released works.³³¹ Proponents respond that concerns regarding the market for other works are not material when analyzing the fourth fair use factor.³³² NTIA agrees that

³²⁵ See *EFF Class 23 Comments* at 7 (“The portion of a game that must be modified to enable play after server shutdown is a very small portion of the overall software.”).

³²⁶ *ESA Class 23 Comments* at 15 (“Such wholesale copying of the copyrighted work (whether it be, for example, the computer program that performs an authentication check or the highly-expressive video game which the access controls are intended to protect) should be disfavored if all or a substantial portion of the work is copied.”).

³²⁷ See *EFF Class 23 Reply Comments* at 11 (“The touchstone of the third factor is that the user copies no more than necessary to achieve a favored purpose. Modifying a game to use a new server (or to eliminate a server requirement) fulfills this criterion because the goal is to preserve the experience of the game unchanged, and not to alter it.”).

³²⁸ See *EFF Class 23 Comments* at 8 (“In many cases, developers abandon a game when sales have already declined to the point where operating a server is no longer financially viable. Harm to the market for a work must vanish when the work is no longer sold.”).

³²⁹ Compare *ESA Class 23 Comments* at 19 (“Only after the online community has effectively dried up, do video game publishers decide to take the game’s video game servers offline.”) with *EFF Class 23 Comments* at 3 (discussing the example of Gamespy, a provider of centralized matchmaking servers, whose 2014 dissolution resulted in hundreds of video games being taken offline).

³³⁰ *ESA Class 23 Comments* at 15.

³³¹ *Id.* at 15-16 (describing how circumvention could lead to (1) publishers creating fewer works than they otherwise would have, (2) more piracy through consoles whose TPMs have been circumvented, and (3) lowered demand for future versions of games, as users continue to play their previously purchased versions).

³³² See *EFF Class 23 Reply Comments* at 12 (“ESA asks the Register to consider impact of preserving a game on the market for ‘new video games within a franchise,’ because preservation ‘may cannibalize sales of new releases.’ In other words, ESA contends that copyright law favors rendering a lawful copy of a work nonfunctional (or less functional) in order to drive sales of other works. This is simply incorrect. The fourth fair use factor is concerned with the market for and value of the work at issue, not other works.”).

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.

In discussing the fourth fair use factor, opponents also raise the important issue of video game piracy. Opponents argue that this exemption, in allowing circumvention of certain TPMs on video game consoles, would lead to widespread piracy and the increased posting of articles with instructions for jailbreaking consoles for piracy purposes.³³³ Proponents rebut this contention by offering examples of video games (especially older video games) where the TPMs circumvented reside on the game media and not in the console, and where the TPMs circumvented for authentication are separate from the encryption used to protect the game files themselves.³³⁴ Additionally, proponents argue persuasively that allowing circumvention of TPMs on the older games that would be covered by this exemption would not lead to piracy of newer games.³³⁵ While NTIA agrees that video game piracy is a legitimate concern, NTIA is convinced that allowing circumvention of games and consoles for the purposes of restoring functionality to unsupported games is not likely to contribute significantly to such piracy. It seems likely that the uses contemplated in this proposed class are fair use, and are thus noninfringing.

Turning to adverse effects, proponents emphasize the loss to video game research and preservation that takes place without an exemption, as well as the loss to consumers who no longer have full functionality in the games that they have purchased. Proponents offer examples from archivists and librarians who say their preservation efforts have been stymied due to an inability to circumvent TPMs.³³⁶ Proponents also offer evidence of dynamics in the video game

³³³ See *ESA Class 23 Comments* at Exhibit A (compiling evidence of Internet commentary discussing circumvention of TPMs on video game consoles in order to engage in piracy).

³³⁴ See *EFF Class 23 Reply Comments* at 5-6 (“In many PC games and older consoles, server communications for authentication and matchmaking operate separately from integrity checks. This means that the modifications necessary to restore the game to functionality do not permit the playing of unauthorized copies of games. For example, games that used the now-shutdown Gamespy servers for multiplayer play can be modified to use new servers without removing other access controls.... ESA’s comments assume that the specifics of modern consoles apply to all circumstances in which a user might want to modify a game, which is not the case. The proposed exemption would accommodate the needs of players and archivists, without including modifications made for purposes of infringement.”).

³³⁵ See *id.* at 4. Opponents’ evidence regarding re-release of video games where multiplayer support had been discontinued does not appear to address proponents’ proposed class. Opponents’ examples seem to consist of new or modified works released under the same or similar titles as previous works. As video game publishers presumably offer server support for these new works, they would fall outside of the bounds of the proposed exemption. See *ESA Class 23 Hearing Response* at 2.

³³⁶ See *EFF Class 23 Reply Comments* at 12-14 (“Preserving a game, such as *Phantasy Star Online* for Sega Dreamcast from 2000, arguably the first console-based online role-playing game, is completely impossible at present. The disc for *Phantasy Star Online* for Dreamcast is just that: a piece of plastic on our shelves. We will never be able to preserve this culturally and historically significant game in any way other than its physical form unless an exemption to the DMCA is made. Future generations will not be able to play the first online RPG for consoles. That is a significant cultural loss.”); *Class 23 Reply Comments of the Preservation and Reformatting Section of the Association for Library Collections and Technical Services* at 3-4, Docket No. 2014-07, available at <http://copyright.gov/1201/2015/reply-comments->

industry (including the increasing number of products where even single-player mode requires online access) that have the adverse effect of limiting consumers' uses of legally purchased products.³³⁷

Addressing proposed alternatives to circumvention, proponents rebut opponents' arguments that single player mode or LAN-enabled multiplayer mode are reasonable alternatives to server-supported multiplayer mode.³³⁸ When LAN-enabled multiplayer mode is available, it requires all players and hardware to be on the same local network, which is a significant limitation compared to the global reach afforded by play over the Internet.³³⁹ With regard to researchers and preservationists, opponents argue that video capture is a sufficient alternative to live play.³⁴⁰ For research and preservation purposes, an alternative that removes the interactivity from a fundamentally interactive medium does not seem to be a reasonable one.³⁴¹

Having analyzed the record, NTIA is persuaded that designating an exemption for a class of works that would allow circumvention for the purposes of restoring access to a previously available video game functions will not adversely affect the market for or value of copyrighted works and would provide relief from the harm proponents demonstrated. Additionally, NTIA believes that this use is a noninfringing use that follows the logic of exemptions granted in past proceedings, including the 2010 exemption for dongles.³⁴²

[050115/class%2023/ReplyComments_ShortForm_PARS_Class23.pdf](#) (describing the ways in which video games inform our culture and the cultural loss that would occur if video games from previous eras were no longer playable in the future).

³³⁷ See *EFF Class 23 Comments* at 10; see also *EFF Class 23 Reply Comments* at 9 (listing examples of games, including *Diablo III: Reaper of Souls*, the most recent edition of *Sim City*, *Assassin's Creed 2*, and *Destiny*, where a server connection is always required for gameplay, even in single-player mode).

³³⁸ See *EFF Class 23 Comments* at Appendix, Statement of T.L. Taylor, Massachusetts Institute of Technology and *EFF Class 23 Reply Comments* at 12 (discussing the vibrant, worldwide player community that exists with an Internet connection and which is not accessible to someone playing over a LAN-connection). Indeed, in many cases, the video games in question do not offer LAN-enabled multiplayer mode as an option. *May 20 Hearing Transcript* at 186-87.

³³⁹ See *EFF Class 23 Reply Comments* at 12 ("Internet play can connect a global community of players at nearly any time of day, while LAN play requires a coincidence of players and hardware at the same location—an expensive proposition in terms of coordination and equipment").

³⁴⁰ See *ESA Class 23 Comments* at 17-18 ("As proponents concede, there are a variety of alternatives to circumvention, such as video capture and other non-play alternatives, for archivists, preservationists, and researchers as well. EFF argues that 'this is not an optimal solution.' However, an exemption is appropriate only in the most 'exceptional cases.' The Librarian routinely has refused to grant an exemption where other alternatives, even suboptimal alternatives, are available.").

³⁴¹ See *EFF Class 23 Reply Comments* at 13 ("A game can no more be fully preserved in static video than a classic film in a still photograph. Just as the essence of a film may reside in its use of motion, editing, and audio, the artistry of a game often lies in the experience of play, which cannot be captured in a video.").

³⁴² In 2010, the Librarian granted the dongle exemption using the following wording: "Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered

Accordingly, NTIA suggests the following exemption:

Computer programs in the form of video games, where circumvention is undertaken for the purpose of restoring access to single-player or multiplayer gaming functionality on consoles, personal computers, or personal handheld gaming devices, and where (1) all or nearly all of the audiovisual content resides on the player's local copy of the game; and (2) the developer and its agents have ceased support for such gaming for a period of six months or more.

2. Music Recording Software (Class 24)

Proponents seek the ability to circumvent access controls consisting of the PACE copy protection system, which restricts access to the full functionality of lawfully acquired Ensoniq PARIS music recording software.³⁴³ Proponents argue that the Ensoniq PARIS software and the PACE copy protection system have been obsolete for over a decade and that, without this exemption, they cannot continue to use their legally purchased software.³⁴⁴

NTIA is generally open to supporting exemptions for obsolete, legally purchased software; the situation described by proponents may indeed be an example of the harmful effects of the DMCA's prohibition against circumvention. However, in order to facilitate the issuing of an exemption in this proceeding, proponents need to provide sufficient evidence on the record.³⁴⁵ Unfortunately, proponents did not meet that burden in this case.

Proponents may be correct in claiming that there is no market value to the developer for the PARIS or PACE systems.³⁴⁶ However, evidence of harm to the proponents is sparse. They state that music libraries will no longer be able to provide access to works created using the PARIS system without an exemption, but do not give specific evidence confirming that claim.³⁴⁷ They

obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace.” *2010 Final Rule* at 43,839. In other words, this exemption, like the previous dongle exemption, would allow a party to restore a previously-available functionality in device or work that he or she owns.

³⁴³ *2014 NPRM* at 73,870. One proponent suggests merging Classes 23 and 24 under the single heading “Software – Abandoned TPMs.” See Class 24 Comments of Mike Battilana at 1, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_longform_MBattilana_Class24.pdf. However, NTIA believes that such a merger would likely create an overly-broad exemption, which the evidence in the record would not support.

³⁴⁴ See Class 24 Petition by Richard Kelly (*Kelly Class 24 Petition*) at 2, Docket No. 2014-07, available at http://copyright.gov/1201/2014/petitions/Kelley_Richard_1201_Initial_Submission_2014.pdf.

³⁴⁵ *2014 NPRM* at 73,857.

³⁴⁶ See *Kelly Class 24 Petition* at 3-4.

³⁴⁷ See Class 24 Comments of the Music Library Association at 1, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_Shortform_MLA_Class24.pdf.

assert that the system is obsolete and abandoned,³⁴⁸ but they do not show specific evidence that Ensoniq no longer authenticates software that uses the PACE system. Proponents' only specific evidence is an assertion that Ensoniq stopped issuing response codes in January 2015.³⁴⁹ For their part, opponents assert that PARIS is not obsolete in the first place because it functions with most of the newest operating systems on the market with the appropriate drivers installed, and because older operating systems are still widely available for purchase.³⁵⁰

Without more evidence in the record to address opponents' arguments and bolster supporting claims, NTIA is unable to support the proposed exemption at this time.

G. Software Security and Safety Research (Classes 22, 25, Part of 27)

Proponents, who include a range of scientists and researchers from prominent academic institutions as well as members of the private sector, seek the ability to circumvent access controls on software in order to conduct security research and testing on a variety of platforms.³⁵¹ Proponents have requested an exemption for the following purposes: conducting general good faith security research, testing the safety and security of vehicle software, and researching the security of networked medical devices.³⁵²

³⁴⁸ See Class 24 Petition by Michael Yanoska at 1, Docket No. 2014-07, *available at* http://copyright.gov/1201/2014/petitions/Yanoska_Michael_1201_Initial_Submission_2014.pdf.

³⁴⁹ See *Kelly Class 24 Petition* at 1.

³⁵⁰ See Class 24 Comments of the Joint Creators and Copyright Owners at 3, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-032715/class%2024/Joint_Creators_and_Copyright_Owners_Class24_1201_2014.pdf. Mr. Kelly himself said in his petition that “a number of coders have taken on the responsibility of developing drivers first for Win Xp, then on modern multicore systems, then on Windows Vista, Windows 7, 8 and 9, all while carefully and diligently respecting the PACE copy protection and without ‘reverse engineering’ the PARIS application.” *Kelly Class 24 Petition* at 3.

³⁵¹ The TPMs security researchers claim are at issue include: (1) measures for controlling installation, execution or use such as keys and passwords, external authentication systems and tethering, dongles and installation media, and license and dialog click-through prompts; (2) measures for controlling reading or inspection such as obfuscation, execute-only memory and trusted platform modules, and encryption; (3) measures for controlling modification such as hashes/checksums and digital signatures, or runtime guards and assertion checks; (4) measures for tracking such as watermarks and external monitoring; and (5) ancillary measures such as TPMs on other protected works such as DVDs or e-Books. See Class 25 Comments of Matthew Green et al., (*Green Class 25 Comments*) at 6-10, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_Green_Class25.pdf. However, proponents acknowledge that the not every technical measure will qualify as a TPM under § 1201(a)(3)(B). *Id.* at 5.

³⁵² See *Green Class 25 Comments*; see also Class 22 Comments of the Electronic Frontier Foundation (*EFF Class 22 Comments*), Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_longform_EFF_Class22.pdf; see also Class 27 Comments of Coalition of Medical Device Researchers, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_longform_Coalition_of_Medical_Device_Researchers_Class27.pdf.

These proposed classes are new to the Section 1201 proceeding, and serve as further examples of the DMCA's prohibition against circumvention being invoked to protect non-copyright interests. While proponents seek the ability to perform good-faith security research, opponents generally do not express concerns about piracy or otherwise unlawful distribution of their copyrighted works. Instead, the opponents' main concern is that exemptions could compromise the safety or security of their systems, particularly in the absence of a requirement that researchers disclose their findings to the software publisher prior to publication.³⁵³

Opponents further argue that an exemption should not be granted without reference to other laws such as the Computer Fraud & Abuse Act (CFAA), 18 U.S.C. § 1030, stating that in order to avoid conflict with or undermining of existing law, the exemption should ensure compliance with other laws.³⁵⁴ NTIA emphasizes that exemptions granted pursuant to this rulemaking do not, and are not capable of, legalizing acts that are unlawful under other statutes.³⁵⁵ If granted, an exemption would not preclude liability under laws such as the CFAA.³⁵⁶

After reviewing the record, NTIA is convinced that good faith security researchers and academics are currently being deterred from engaging in noninfringing activities due to the threat of litigation under Section 1201.³⁵⁷ In turn, this is having an adverse impact on criticism,

³⁵³ See Class 25 Comments of BSA – The Software Alliance (*BSA Class 25 Comments*) at 2, Docket No. 2014-07, available at [http://copyright.gov/1201/2015/comments-032715/class%2025/BSA The Software Alliance Class25 1201 2014.pdf](http://copyright.gov/1201/2015/comments-032715/class%2025/BSA%20The%20Software%20Alliance%20Class25%201201%202014.pdf) (expressing concern about the proposed exemption's lack of disclosure policy and arguing for a provision that would require notice to the publisher(s) before public disclosure).

³⁵⁴ See *BSA Class 25 Comments* at 2, 5. Under the CFAA, the unauthorized access, or exceeding authorized access, to a protected computer violates the statute.

³⁵⁵ See Transcript of May 26, 2015, Hearing on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Section 1201 – Digital Millennium Copyright Act (*May 26 Hearing Transcript*) at 148-49, Docket No. 2014-07, available at <http://copyright.gov/1201/2015/hearing-transcripts/1201-Rulemaking-Public-Roundtable-05-26-2015.pdf> (“[T]he DMCA was intended to protect devices that contained code or books or what have you that have been legitimately purchased that you’re trying to prevent extraction of, reproduction of in violation of the Copyright Act. It’s not intended to be a CFAA supplement. And, again, as a technical matter, that’s rarely the way. You have to break something else if it’s somebody else’s system, violate the CFAA before you can get to the copyrighted code. And that’s rarely the way that copyrighted or otherwise protected material is stolen because of a hack.”).

³⁵⁶ NTIA notes that CFAA claims are at times brought in conjunction with Section 1201 DMCA violations. See *Sony Computer Entm’t America, LLC v. Hotz*, No. CV110167, 2011 WL 347137 (N.D. Cal. Jan. 27, 2011). However, to provide clarity, NTIA includes a provision in our proposed exemption that notes the continuing applicability of other relevant laws, such as the CFAA.

³⁵⁷ See, e.g., Class 25 Comments of Mark Stanislav (*Stanislav Class 25 Comments*), Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_Stanolav_Class25.pdf (“The DMCA has damaged both my research and my quality of life: in the past the DMCA has been wielded as a weapon against me by companies that were unreceptive to my attempts to engage with them to confidentially disclose and help fix security flaws that I found in products for use by small children.... The act of analyzing firmware to verify its safety for consumer use often lands a researcher like me in a legal nightmare.”); Class 25 Comments of Dr. Salvatore J. Stolfo, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_Stolfo_Class25.pdf (“[I] currently wish to pursue more research in the areas of insecure embedded devices, such as the insecure routers that constitute the communication substrate of the internet

scholarship, and research.³⁵⁸ As security breaches and instances of hacking populate the news with increasing frequency, it is essential that security researchers have the ability to conduct necessary research in order to identify and notify publishers and the public *before* the vulnerabilities lead to massive breaches or exploitations.³⁵⁹ Security researchers from universities around the world and leading security companies agree, stating that “government and corporate systems, consumer products, financial transactions, and national security are less secure as a result of the unperformed research.”³⁶⁰ More security research will lead to more secure networks and encourage responsible practices.³⁶¹

Although many factors favoring and disfavoring an exemption for security research largely fall outside the purview of copyright law, to the extent that there is a copyright interest, NTIA believes that security research is noninfringing and constitutes fair use.³⁶² As recognized by the

and government networks, however, I have been advised by attorneys that some of this research may run afoul of DMCA Section 1201. As such, I have not yet pursued this research, despite its necessity and potential to improve information security of components and systems, which is clearly in the best interests of the national to secure its critical infrastructure.”); *May 26 Hearing Transcript* at 12-13 (Researcher Matthew Green states: “In my opinion, the Section 1201 was never intended to prevent security researchers from publishing their results. In the moment though, when you’re a penniless grad student and somebody is presenting you with a possibility of a lawsuit you can’t possibly afford, it’s hard to argue about the merits of a case or the intent of a law. It’s more tempting to simply comply and hide a serious vulnerability from public view.”).

³⁵⁸ See 17 U.S.C. § 1201(C)(iii) (2012).

³⁵⁹ See, e.g., *Green Class 25 Comments* at 23 (“The importance of improving the security of these systems has never been more apparent as evidenced by the recent high-profile breach at Sony, and the seemingly endless list of credit card systems that have been compromised.”); Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway - With Me in It*, *Wired*, July 21, 2015, available at <http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/> (verifying the threat of remotely hacking a vehicle’s ECU to take control of the vehicle’s functionality).

³⁶⁰ See *Class 25 Comments* of Gavin Anderson, et al., Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_AndresenEtAl_Class25.pdf (Letter signed by researchers from leading universities around the world and companies including Bitcoin, Microdesic, Unipay Technologies, and Symantec). See also *Class 25 Comments* of Dr. Ian Brown, et al., Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_Brown_Class25.pdf (Professors from the University of Oxford, the University of Cambridge, and University College London state that the exemption “will better... defend national and international security interests, critical infrastructure, and the economies of both the United States and its trusted allies.”).

³⁶¹ See *Class 25 Comments* of the Internet Association (*Internet Association Class 25 Comments*), Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_InternetAssociation_Class25.pdf (“[I]f the exemption is granted, security researchers inside companies will be better able to defend corporate intellectual property assets, as well as the data of the consumers who trust us with their information. Similarly, external security researchers would more readily report any malfunctions, flaws or vulnerabilities to us in order to assist us in improving our offerings – a practice we supports and financially reward through bug bounty programs.”).

³⁶² See *EFF Class 22 Comments* at 7 (“This research is an archetypical fair use codified in Section 107, undertaken to enhance public knowledge about the functioning of vehicles to which hundreds of millions of American trust their lives. In the course of engaging in security and safety research, an individual may copy the code (typically onto a general-purpose computer for analysis), modify the code (for example, to detect or patch a security vulnerability or safety issue), and distribute the code as part of scholarly discourse. Such discourse could include criticism of the

Register in prior exemptions, uses relating to security research are likely to be noninfringing.³⁶³ Section 117 of Title 17 also supports this conclusion.³⁶⁴

Statutory Factors

Proponents have addressed the statutory factors to be considered in this rulemaking, and assert that each of them weighs in favor of granting the proposed exemption. First, the availability of copyrighted works for security research is limited absent an exemption. Proponents claim that a general exemption for good faith security research “will increase the number of copyrighted works available for study by superseding the existing patchwork of prior, narrowly-defined good faith security research exemptions.”³⁶⁵ Further, the risk of liability is, in fact, precluding research from being conducted due to legal ambiguity and litigation risks.³⁶⁶

code’s flaws, positive scholarship regarding its approach to security or safety, or reporting on matters of public interest, including vulnerabilities and bugs.”).

³⁶³ See *2010 Final Rule* at 43,833 (“[T]he factors set forth in 17 U.S.C. 107 tend to strongly support a finding that such good faith [security vulnerability] research constitutes fair use. The socially productive purpose of investigating computer security and informing the public do not involve use of the creative aspects of the work and are unlikely to have an adverse effect on the market for or value of the copyrighted works itself.”); Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket. No. RM 2005-11, Final Rule, 71 Fed. Reg. 68,472, 68,477 (Nov. 27, 2006) (*2006 Final Rule*), available at <http://www.copyright.gov/fedreg/2006/71fr68472.pdf> (granting an exemption for good faith security testing for sound recordings and associated audiovisual works contained on a compact disc protected by TPMs creating security vulnerabilities on personal computers).

³⁶⁴ 17 U.S.C. § 117 provides further limitations on the exclusive rights of copyright owners of computer programs, stating that it is not an infringement for the owner of a copy of a computer program to make a copy of that program when (1) created as an “essential step in the utilization of the computer program” or (2) the new copy is created for archival purposes only. It also permits the owner or lessee of a machine to make or authorize the making of a copy of a computer program for purposes of maintenance and repair, with limitations. See 17 U.S.C. § 117(a), (c) (2012). To the extent these actions addressed in the statute are necessary to conduct security research, Section 117 provides further support to conclude that the use is likely to be noninfringing. NTIA rejects the argument that the owners of a lawfully purchased vehicle are not the owners of a copy of the software installed in that vehicle’s ECU. *Supra* notes 258-265 and accompanying text.

³⁶⁵ *Green Class 25 Comments* at 22-23; see also *Security Research Class 25 Comments* at 8 (“This proposed exemption would ensure a safer environment for security research that would stimulate production of more works. More copyrighted works would be created, and the work would be of even higher caliber”); *Internet Association Class 25 Comments* at 1 (“[I]f the exemption is granted, security researchers inside companies will be better able to defend corporate intellectual property assets, as well as the data of the consumers who trust us with their information.... In brief, granting this exemption would be a significant step toward improving information security in this economy.”).

³⁶⁶ See *Green Class 25 Comments* at 23 (“The risk of liability under Section 1201 when performing security research in educational contexts forces researchers to limit students involvement and can push risk-averse universities from such research. Because the individuals conducting security researchers [sic] are often graduate students with few resources, professors limit their involvement to limit their liability.”); *Internet Association Class 25 Comments* (“The DMCA currently suffers from ambiguities regarding the legality of this type of necessary and everyday security testing performed by or at the request of responsible companies such as ours. Our business planning is meaningfully damaged by legal ambiguities such as those in the DMCA. The DMCA exposes us and our employees to additional legal risks as we strive to protect our customer’s safety and our own intellectual property assets and

With regard to the impact that the prohibition on circumvention of access controls has on criticism, comment, news reporting, teaching, scholarship, or research, proponents claim that

[a]cademic and amateur security researchers, commonly known as “white hat” researchers, are negatively affected by a prohibition on circumvention of technological measures in a variety of contexts. Good faith security research includes criticism, commentary, news reporting, teaching, scholarship, and research. All aspects of security research, from scholarship, to teaching, to testing, to commenting, criticizing, and reporting, are disincentivized by the current gaps and ambiguities in Section 1201’s exemptions. The resulting chilling effects inhibit key security research, hindering the security of critical information infrastructure.³⁶⁷

Lastly, proponents claim that a general exemption for good faith security research will create a positive net effect on the market for software and devices.³⁶⁸ The goal of good faith security research is not promoting the distribution of illegal works or other illicit behavior; instead, the record shows that a researcher generally manipulates the code of the copyrighted work in order to test for vulnerabilities and glitches.

In response to the Copyright Office’s request for “specific examples of acts of security research that have been foregone or delayed due to the current lack of the proposed exemption,”³⁶⁹ proponents cited many instances in which the DMCA has hindered research, including efforts to assess the security of microphones, motor vehicles, household appliances, surveillance cameras, public safety communications equipment, financial services, government and commercial information systems, electronic voting systems, and medical devices.³⁷⁰ They state that legal counsel regularly advises researchers “that the DMCA is an unclear statute and that undertaking any such research exposes the researcher to legal risk,” and that they “usually counsel

goodwill.”); *May 26 Hearing Transcript at 51* (“The questions that we’re considering today at root deal with a type of frivolous litigation. They are an attempt to mitigate disclosure and conversation around existing flaws that may impact consumers, the safety of our economy, the safety of our critical infrastructure. And as such the request that we’re making of this esteemed panel is to help curb the frivolous litigation that arises as a consequence of Section 1201.”).

³⁶⁷ *Green Class 25 Comments at 23.*

³⁶⁸ *Id. at 24.*

³⁶⁹ *2014 NPRM at 73,871.*

³⁷⁰ *See Class 25 Comments of Security Researchers (Security Researchers Class 25 Comments) at 9-10, Docket No. 2014-07, available at <http://copyright.gov/1201/2015/comments>; Stanislav Class 25 Comments at 1; Class 25 Comments of Jay Radcliffe, Senior Security Consultant, Rapid 7 (Rapid 7 Class 25 Comments) at 1, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_Radcliffe_Class25.pdf (“I am confident that I would find serious flaws in some or all of these [medical devices] if the DMCA did not prevent my research. Because of this lack of safety research, as a type 1 diabetic, I feel that using an insulin pump is too unsafe, and I instead self-inject with needles many times daily. I am not alone in this safety assessment: other diabetic security researchers behave similarly.”).*

against continuing the research.”³⁷¹ Last, when the software being researched is protected by a TPM, there are no substitutes for access to the software, and therefore no alternatives to circumvention.³⁷² In sum, the record contains a plethora of evidence demonstrating that Section 1201 is currently preventing important security research from coming to fruition.

Statutory Exemptions

At the time of its enactment, Congress recognized the necessity that the DMCA not deter beneficial security research and included statutory exemptions for reverse engineering, encryption, and security testing.³⁷³ Opponents argue that the existing exemptions are evidence that Congress already contemplated the need for security research exemptions, and that there is no need to grant an additional exemption without the constraints included in the statute.³⁷⁴ However, NTIA is not convinced that Congress intended these provisions to be the only exemptions pertaining to security research.

While these exemptions may, in some circumstances, provide a mechanism through which various research activities can be performed, the record indicates that these three statutory exemptions are not sufficient to obviate the need for a broad good faith security research exemption.³⁷⁵ The statutory exemptions are rigid and require the researcher to fit his or her research project into a specific category prior to circumvention. It is because of these prescriptive

³⁷¹ *Security Researchers Class 25 Comments* at 3-4 (“For example, one of us was investigating the integrity of a secure wireless communication system used by various government agencies. In the course of this investigation, s/he was counseled by an attorney that constructing tools to extract the firmware from a particular vendor’s product in ways not supported by the existing interfaces for the purpose of vulnerability analysis could constitute a violation of the DMCA. This precluded analysis of implementation vulnerabilities and limited the scope of analysis to those vulnerabilities that could be found in the published specifications for the system.”).

³⁷² *See Green Class 25 Comments* at 22 (“In most cases of security research, there are no reasonable alternatives to circumvention. This is because all instances of the software or device under investigation are protected by TPMs, thus no investigation can take place without bypassing a TPM.”).

³⁷³ *See* 17 U.S.C. § 1201(f)-(g), (j) (2012). Proponents also note that the exemption in Section 1201 (i), which permits a *consumer* to investigate code functionality on a privately-owned system in order to determine whether a privacy harm is occurring, further evidences that “Congress specifically contemplated and sought to protect the public from malfunctioning, flawed, or vulnerable code that harms consumers.” *Security Researchers Class 25 Comments* at 5; 17 U.S.C. § 1201 (i). However, this exemption is not sufficient as it only applies to consumers, who might lack the technological skills needed to engage in the type of inquiry that Section 1201(i) expressly authorizes. *See Security Researchers Class 25 Comments* at 5.

³⁷⁴ *See BSA Class 25 Comments* at 2-3 (“This proposed class of works is unmoored from virtually any of the reasonable constraints Congress placed on good faith security research in 17 U.S.C. § 1201(j)... [T]he proposed class of works disregard the directives that Congress made in section 1201(j)[.]”).

³⁷⁵ *See Green Class 25 Reply Comments* at 10 (“While Section 1201(j) is evidence of Congress’s general concern to permit circumvention under appropriate circumstances for purposes of security testing, the fact that exemptions closely related to 1201(j) have been granted in the past, shows that the limitation in the statutory exemptions should not limit the grant of a triennial exemption. The limitations are merely reflective of the technical specifics that existed in 1998, and there is no indication that Congress intended the exemptions to fall behind changing technology.”).

requirements, a lack of clarity, uncertainty over litigation, and other ambiguities that proponents seek an exemption.³⁷⁶ Accordingly, an exemption granted by the Librarian would not contradict the existing exemptions.³⁷⁷ Rather, the proposed general good faith security exemption would work in harmony with Sections 1201(f), (g), and (j) to encourage essential research.

The Reverse Engineering Exemption – 17 U.S.C. § 1201(f)

The statutory reverse engineering exemption allows a person to circumvent a technological protection measure 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.³⁷⁸ Interoperability is defined as “the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged.”³⁷⁹

The particular issue with this exemption is that not all security research has the “sole purpose” of improving interoperability.³⁸⁰ One of the proponents noted that, while some research may be related to the improvement of interoperability,” research often has other purposes in addition to (or exclusive of) interoperability.”³⁸¹ For example,

[s]ome crucial security research may be broadly construed to improve the interoperability of computer programs by exposing security flaws, incentivizing companies to repair those flaws, and thereby improving the suitability of the programs for interoperation with the other programs. However, the broader aims of good faith security research include publication, teaching students in security research to understand the access controls they are working with, and improving the security of all software and devices.³⁸²

³⁷⁶ *Id.* at 19 (“Their overly narrow scopes, restrictions on research, restriction on dissemination of information, authorization requirements, reliance on multi-factors tests, and other infirmities mean that the built-in exemptions fails to provide the certainty necessary for researchers to pursue projects involving TPMs.”).

³⁷⁷ *Security Researchers Class 25 Comments* at 4 (“Granting this requested exemption cleanly updates and clarifies the scope of statutorily allowed research in Sections 1201(g), (f), and (j) in light of the ambiguities created by new types of information security threats facing companies, consumers, and our country’s national security.”).

³⁷⁸ 17 U.S.C. § 1201(f) (2012).

³⁷⁹ *Id.*

³⁸⁰ *Green Class 25 Comments* at 20.

³⁸¹ *Id.*

³⁸² *Id.*

In the case of networked medical devices, researchers engage in reverse engineering to discover underlying vulnerabilities in the underlying source code.³⁸³ Section 1201(f) is inapplicable as it applies when the researcher engages in reverse engineering when developing interoperable software, rather than analyzing vulnerabilities of existing software.³⁸⁴ However, as proponents state, “there is no indication that Congress intended Section 1201(f) to be the only permissible act of reverse engineering.”³⁸⁵ Opponents claim that reverse engineering that allows access to source code will “likely increase the number of knock-off products” and lead to a “black market” of illegitimate devices.³⁸⁶ However, substantive evidence of the likelihood of such dangers was not presented.

The Encryption Research Exemption – 17 U.S.C. § 1201(g)

The second exemption is specific to encryption research, and requires researchers to meet and comply with various conditions to qualify for the exemption.³⁸⁷ For example, researchers must obtain a copy of the work lawfully, “make a good faith effort to obtain authorization before circumvention,” show that circumvention is “necessary to conduct such encryption research,” and ensure that the research “does not constitute infringement under this title or a violation of applicable law other than this section.”³⁸⁸ But even assuming compliance with all those parameters, the statute enumerates various factors to determine “whether a person qualifies for the exemption,” including:

- Whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under the copyright act or a violation of other applicable laws, including a violation of privacy or breach of security;
- Whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology; and

³⁸³ See Class 27 Comments of Collation of Medical Researchers at 4, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments020615/InitialComments_longform_Coalition_of_Medical_Device_Researchers_Class27.pdf (“Depending on the specific form of research, researchers may wish to access this code alone, or they may wish to decompile the object code to reveal the underlying source code, or the programming language used by developers when coding the device.”).

³⁸⁴ *Id.* at 15.

³⁸⁵ *Id.*

³⁸⁶ See Class 25 Comments of the Advanced Medical Technology Association (*AdvaMed Class 25 Comments*) at 6, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments032715/class%2025/AdvaMed_Class25_1201_2014.pdf.

³⁸⁷ 17 U.S.C. § 1201(g) (2012).

³⁸⁸ *Id.*

- Whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research, and the time when such notice is provided.³⁸⁹

Proponents have demonstrated that these rigid *ex* and *post ante* considerations deter independent research from the academic community and adversely harm those that might lack reliable access to legal representation in the event of litigation, even if their work is lawful.³⁹⁰ In fact, the record contains numerous statements from researchers expressing their frustration at their inability to conduct security research under this exemption.³⁹¹ More notably, the record contains evidence that some researchers have already identified flaws and vulnerabilities but have not revealed them or otherwise announced them due to fear of liability under the DMCA.³⁹²

In addition, proponents believe that this statutory exemption contains “numerous ambiguities and requirements that do not provide sufficient clarity as to the legality of good faith security research.”³⁹³ Some research is conducted by students seeking to gain experience and not necessarily to “advance the state of knowledge in the field of encryption technology” as required by the statute.³⁹⁴ Further, there is a wide range of security researchers from different professional and academic backgrounds, not all of whom necessarily fall under the classifications of the statute.³⁹⁵ Simply put, the record indicates that the lack of clarity surrounding this exemption is deterring essential encryption research.

³⁸⁹ *Id.*

³⁹⁰ See *May 26 Hearing Transcript* at 15-16 (“[A]s we’ve asked the office to do several times in the past and as the office and librarian have done, we’re asking for some additional clarity to make clear for folks up front before they start a project that, if they’re proceeding in good faith, that they’re doing the right thing, they’re doing this only for security testing or security research and they’re not doing it to facilitate any sort of copyright infringement, that they’re free and clear.”).

³⁹¹ See *id.* at 17 (“[I would advise a researcher that he should be nervous about the DMCA] because a lot of the provisions in this law are ambiguous and we don’t ultimately know how they would be applied.”).

³⁹² *Green Class 25 Comments* at 22 (“In many cases, developers and copyright holders attempt to leverage Section 1201 against researchers to conceal security vulnerabilities rather than fixing them.”).

³⁹³ *Id.* at 20-22.

³⁹⁴ To take advantage of Section 1201(g), the research must “advance the state of the knowledge in the field of encryption technology.” 17 U.S.C. § 1201(g) (2012). Proponents argue that security research projects are not always conducted with that goal in mind, noting that “some projects are conducted to provide students with valuable experience working on real systems.” *Green Class 25 Comments* at 20. Due to the legal uncertainty surrounding the provisions, it is not clear whether this use is permitted under the exemption. *Id.*

³⁹⁵ *Green Class 25 Comments* at 21 (“Although many working in security research are professionals, there is much valuable work being done in this space by amateurs.”).

The Security Testing Exemption – 17 U.S.C. § 1201(j)

The statutory exemption in Section 1201(j) only allows security testing that requires access to “a computer, computer system, or computer network” with the authorization of the owner of the “computer, computer system, or computer network.”³⁹⁶ However, proponents argue that this exemption is often inapplicable to modern realities of security research.

First, the Copyright Office has narrowly defined what qualifies as a “computer, computer system, or computer network.”³⁹⁷ Much of the research that proponents are conducting is on newer platforms that might not fit within the guidelines first published five years ago.

Second, researchers are required to obtain prior authorization from the owner of the computer, computer system or computer network. The proponents have identified multiple obstacles in satisfying this requirement. The act of identifying the owner can be a “complex factual determination” and “in many cases is impossible.”³⁹⁸ A researcher doing wholly separate research that incidentally discovers a specific vulnerability may not have known to seek authorization before commencing his or her work.³⁹⁹ Further, fear of public disclosure of security vulnerabilities may incentivize owners to withhold this authorization; upon receiving a request for authorization, some owners may even initiate legal action.⁴⁰⁰

Third, even if the researcher manages to satisfy these initial requirements, the statute also requires consideration of additional factors, as in the encryption research exemption. Section 1201(j)(3) requires consideration of the following:

- Whether the information derived from the 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 testing is used in a manner that does not facilitate infringement or violates any other applicable law.⁴⁰¹

The first provision is detached from the current reality of software vulnerabilities and security research in general. The factor centers on whether the activity is solely for the benefit of

³⁹⁶ 17 U.S.C. § 1201(j) (2012).

³⁹⁷ *Green Class 25 Comments* at 21 (citing *2010 Final Rule* at 43,832-33).

³⁹⁸ *Id.* at 21.

³⁹⁹ See *May 26 Hearing Transcript* at 106-07 (discussing the case of the so-called “accidental researcher” who finds a vulnerability in the course of investigating a different issue).

⁴⁰⁰ *Green Class 25 Comments* at 18, 22.

⁴⁰¹ 17 U.S.C. § 1201(j)(3) (2012).

the computer's owner or operations which makes this exemption extremely difficult to apply to the researchers at large today. Proponents note:

Many research projects may lead, for example, to the release of information on how the owner or operator of a computer, computer system, or computer network failed to properly secure a computer system, or other outcomes that may benefit the public, but not the owner.⁴⁰²

Opponents argue that this exemption is sufficient to cover the desired uses of proponents and Congress carefully crafted this exemption to provided proper balance. NTIA agrees that some of the examples identified on the record may be covered under the existing statute. However, the widely reported mass uncertainty over these exemptions, combined with the potentially unrealistic requirements and restrictions, necessitate a complementary exemption for general security research. The Copyright Office has not limited itself to the confines of Section 1201(j) when evaluating past petitions relating to security testing, and should follow suit in this proceeding.⁴⁰³

Alleged Risks Outside Copyright Infringement

Opponents cite a variety of concerns over the revealing of security vulnerabilities and the potential for regulatory compliance issues. Many of these concerns may represent legitimate issues for both manufacturers and the public at large, and they deserve consideration in the proper fora. However, in the context of this proceeding, these claims are simply not *copyright* concerns. The technological protection measures at issue in the Section 1201 proceeding are access controls implemented to deter *copyright* infringement in the digital environment. While most of the works at issue are entitled to copyright protection, the TPMs controlling access to those works have, in many cases, been deployed not to protect such works from piracy, but rather to ensure system integrity and, at times, to enforce a business model unrelated to copyright.⁴⁰⁴ While some opponents address these tangential concerns in the context of the fifth

⁴⁰² *Green Class 25 Comments* at 22.

⁴⁰³ See *2006 Final Rule* at 68,477 (“Copyright owners opposed the proposed exemption primarily on the ground that they believe there already exists a statutory exemption that permits circumvention of access controls for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network. [internet citation omitted] But while it appear that this statutory exemption may permit circumvention n in cases such as those involving MediaMax and XCP, it is not clear whether that provision extends to such conduct. In light of that uncertainty and the seriousness of the problem, the Register recommends that the librarian designate a class of works consisting of sound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigation, or correcting such security flaws or vulnerabilities.”).

⁴⁰⁴ See *Class 22 Comments of General Motors (GM Class 22 Comments)* at 28, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%2022/General_Motors_Class22_1201_2014.pdf (“GM’s TPMs are strategically designed and implemented to protect the vehicle occupant safety, which is out highest priority, as well as to thwart illegal activities.”).

statutory factor examined in this proceeding, NTIA reiterates its opinion that the fifth factor should not be used to engage in non-copyright policymaking, which is beyond the authority and expertise of the agencies involved in this rulemaking.⁴⁰⁵ In its deliberations, the Copyright Office should, as previously mentioned, focus on questions relevant to copyright law rather than on unrelated matters, important as those issues may be.

In addressing opponents' concerns below, NTIA does not seek to minimize the importance of such risks, or assert that they should not be addressed by regulations or legislation. However, NTIA hopes that this discussion will further the debate in a more appropriate venue for addressing these risks.

Application of Exemption to Vehicles

Proponents of Class 22 requested a good faith security research exemption for “motorized land vehicles.”⁴⁰⁶ Opponents oppose the exemption for vehicle security research in its entirety.⁴⁰⁷ The opponents for Class 22 are primarily concerned with the potential for the exemption to enable individuals to more easily violate non-copyright regulatory standards and compliance measures.⁴⁰⁸ They argue that publically distributing code relating to the ECUs that control critical safety and security systems would impact “the automobile safety, security and regulatory landscape,”⁴⁰⁹ affecting everything from consumer privacy to vehicle emission standards.

⁴⁰⁵ See *GM Class 22 Comments* at 18.

⁴⁰⁶ See Initial Petition of the Electronic Frontier Foundation Vehicle Software Security and Research, Docket No. 2014-07, available at http://copyright.gov/1201/2014/petitions/Electronic_Frontier_Foundation_3_1201_Initial_Submission_2014.pdf. As discussed in Class 21, above, for the sake of regulatory consistency, NTIA relies on the definition of “motor vehicles” found in 49 U.S.C. § 13102. Agricultural machinery is left intentionally broad, to ensure that all devices identified by proponents are included, recognizing that the definition of such class of machines varies.

⁴⁰⁷ Opponents argue that vehicle security research is infringing because proponents have not demonstrated that the owner of a vehicle is also the owner of the software within the vehicle. See *GM Class 22 Comments* at 8-9. While the licensing agreement does not explicitly transfer the title of ownership in the software itself, the proponents have made a persuasive argument that the owner of a vehicle is also the owner of a copy of the software within the vehicle. NTIA rejects GM and John Deere’s assertions that the lawful owner of a vehicle is not entitled to uses under Section 117(a) due to a lack of ownership.

⁴⁰⁸ Opponents also argue that, using knowledge procured from the public disclosure of vulnerabilities, individuals will consequently implement the findings through modification in attempts to “fix” the problem. These concerns are better addressed in the discussion for Class 21, which addresses software repair and modifications. The security research exemption would only permit the actions necessary to identify vulnerabilities through security research. See *supra* Class 21: Vehicle software – diagnosis, repair, or modification, page 49. Further, opponents inaccurately conflate the two exemptions with respect to users. They state that the automobile enthusiast would be the ones conducting research on the vehicles “out of curiosity” or “as a hobby.” *John Deere Class 22 Comments* at 6. NTIA understands, rather, that the researcher would consist of academics, computer scientists, and anyone that sought to discover security vulnerabilities or flaws.

⁴⁰⁹ *GM Class 22 Comments* at 3.

Opponents' primary concerns relate to the exemption making their own systems less secure and safe. However, proponents have readily identified many instances in which security research has led to *more* secure systems and reduced risk.⁴¹⁰ Opponents also argue that the exemption would disrupt current security research programs conducted through the auto manufacturers themselves. For example, opponents cite the Collaborative Safety Research Center at Toyota and the Honda Developer Studio.⁴¹¹ GM also engages third party researchers to identify and address security vulnerabilities.⁴¹² NTIA encourages manufacturers to continue investing in research and to further develop programs such as these.

Security research, however, should not be the exclusive purview of those manufacturing and selling a product.⁴¹³ Proponents have cited multiple instances where the existence of in-house security testing programs has been insufficient to satisfy all security needs. Recent examples in the news serve as evidence of such program shortcomings.⁴¹⁴ This past July, Wired published a story identifying an serious vulnerability in the electronic control systems in Chrysler vehicles. Two researchers were able to remotely hack the ECU in a 2014 Jeep Cherokee, controlling critical vehicle functions, such as acceleration, from miles away and gaining access to GPS coordinates, enabling surveillance.⁴¹⁵ Fiat Chrysler Automobiles (FCA) followed this discovery

⁴¹⁰ *May 19 Hearing Transcript* at 16 (“By reverse engineering code and some important ECUs [sic], they identified several vulnerabilities in the vehicle, for example, the Bluetooth stack and the cellular components... that allowed them to inject the message into a vulnerable vehicle from anywhere in the country. As they showed earlier, with this method, they would follow this by remotely locking up the brakes on these vehicles or cause other safety critical features without the drive doing anything from miles away.”).

⁴¹¹ See Class 22 Comments of the Association of Global Automakers (*Global Automakers Class 22 Comments*) at 5, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%2022/Association_of_Global_Automakers_Class22_1201_2014.pdf.

⁴¹² *May 19 Hearing Transcript* at 30.

⁴¹³ “We have speculation on the other side based on a couple myths that have been rejected in the computer security world about the idea that you can build secure systems by keeping them isolated from independent scrutiny or the fiction that there malicious hackers who are waiting for legitimate researchers to find vulnerabilities and exploit them, both of which are speculation and myths in the security research world.” *Id.* at 14.

⁴¹⁴ More recently, the vulnerabilities in the OnStar system and the new mobile application, downloaded by more than 3 million people, were publically revealed. While the fix was relatively easy for GM to make through a server software update, it only represents the growing risk to vehicular safety. See Jim Finkle and Bernie Woodall, *Research Says Can Hack GM's OnStar App, Open Vehicle, Start Engine*, Reuters, July 30, 2015, available at <http://www.reuters.com/article/2015/07/30/us-gm-hacking-idUSKCN0Q42FI20150730>. Senator Edward Markey released a report earlier this year regarding the lack of cybersecurity and privacy protection measures taken by a number of automobile manufacturers. See generally Staff of Sen. Edward J. Markey (D-Massachusetts), *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk* (2015), available at http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

⁴¹⁵ See Andy Greenburg, *Hackers Remotely Kill A Jeep on the Highway – With Me In It*, Wired, July 22, 2015, available at <http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>.

with a recall for 1.4 million potentially vulnerable vehicles.⁴¹⁶ The researchers notified FCA months before Wired published the story and worked with FCA to create a patch, which was released to the public. This is a promising sign that an exemption benefiting security researchers would assist manufacturers in discovering and fixing vulnerabilities in a responsible manner.

While opponents might argue that the above examples actually favor their view that anyone can hack a car, NTIA emphasizes that uses outside of security research, *e.g.*, for nefarious purposes, would not be permitted under this exemption. NTIA rejects opponents' claims that by "removing automobile manufacturers from research programs, independent researchers will be free to further any agenda in the name of security."⁴¹⁷ Any action that is illegal under laws outside Title 17 would remain illegal with an exemption in place.

Networked Medical Devices

Class 27 proponents request an exemption to allow for circumvention of TPMs on software contained in medical devices such as insulin pumps.⁴¹⁸ They argue there has been a significant lack of research in this area due to stringent regulations, noting that as much as 40 percent of computer code in medical devices remains untested by independent security experts.⁴¹⁹ With an exemption, proponents argue they will be better equipped to discover vulnerabilities and identify vulnerable devices and designs.⁴²⁰ Opponents claim that the exemption cannot be granted as it would conflict with the FDA's ability to regulate the devices.⁴²¹ They assert that an exemption would detrimentally affect patient health and privacy concerns.⁴²² Opponents also identified the medical device recertification process as a potential area of concern.⁴²³ Proponents, however,

⁴¹⁶ Consumer Reports, *Protect You Chrysler, Dodge, or Jeep From Hacking, Fiat-Chrysler Issues Software Updates for 1.4 Million Vehicles*, July 24, 2015, available at <http://www.consumerreports.org/cro/news/2015/07/protect-your-chrysler-dodge-or-jeep-from-hacking/index.htm>.

⁴¹⁷ *Global Automakers Class 22 Comments* at 7.

⁴¹⁸ As discussed above, NTIA addresses the two separate issues that arise in the requested Class 27 exemption separately: (1) information retrieval, addressed in Part II.E.2; and (2) security research, addressed here. As noted above, NTIA supports a broad security research exemption irrespective of the device within which the software is contained.

⁴¹⁹ *See Rapid 7 Class 25 Comments* at 1.

⁴²⁰ *Id.*

⁴²¹ *See Class 27 Comments of LifeScience Alley* at 2, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%2027/LifeScience_Alley_Class27_1201_2014.pdf.

⁴²² *See Class 27 Comments of the Medical Device Innovation, Safety, and Security Consortium*, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%2025/Medical_Device_Innovation_Safety_and_Security_Consortium_Class25_1201_2014.pdf.

⁴²³ *See Class 27 Reply Comments of Jay Schulman*, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-032715/class%2027/Jay_Schulman_Class27_1201_2014.pdf ("When security issues are discovered in medical devices, it could result in the device having to go through recertification with the FDA. That process could take months to years to complete while the vulnerability in the device remains.

argue that the TPMs are not currently deterring bad actors, but only disadvantaging “good” researchers in their race against “black hat” hackers to discover these security flaws. NTIA is inclined to agree with proponents. To the extent that the exemption touches on issues under existing regulatory regimes, NTIA defers to the respective agencies to address concerns unrelated to copyright.

Proposed Disclosure Policy

Opponents request that, if the Copyright Office chooses to recommend an exemption for security research, the exemption require researchers to give notice to rights holders before public disclosure of a security vulnerability, and to mandate that researchers receive permission prior to conducting research.⁴²⁴ There are many examples of positive interactions between a researcher that has identified a flaw or vulnerability and the owner of the affected software.⁴²⁵ Further, some companies encourage outside research by offering “bounties” or conducting vulnerability reward programs for finding security flaws in their systems.⁴²⁶

However, there is a significant amount of evidence that not all vendors are as receptive to external security vulnerability research. Proponents of the class felt uncomfortable with the Copyright Office crafting an exemption that mandated that the researcher notify the copyright owner of the software after discovering a flaw or security issue. While many researchers practice responsible notification practices when contacting vendors, it may not be the most effective way to fix the flaw in all circumstances. At times, proponents note, the company that distributes the program with the security flaw has no mechanism to identify and address security vulnerabilities.⁴²⁷ Problems include the lack of a public-facing portal to allow researchers to

While Google has a 60 day notice period once they notify a vendor of a security bug, a medical device manufacturer can’t patch their software or hardware in the same way Google, Microsoft, or Adobe can.”).

⁴²⁴ See Class 25 Reply Comments of BSA – The Software Alliance at 5, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments032715/class%2025/BSA_The_Software_Alliance_Class25_1201_2014.pdf.

⁴²⁵ See *May 26 Hearing Transcript* at 52-53 (“[I]n my experience, there are two types of companies. Some companies are very receptive to receiving this type of [security research] information; in fact, they welcome it. There are sophisticated entities, such as Facebook and Google and Tesla who have bug bounty programs where they compensate, in fact, researchers asking them to help with securing their products. And so there’s this affirmative solicitation. They have processes in place with a clear reporting mechanism on their websites, for example, and internal identifying personnel to engage with these conversations.”).

⁴²⁶ See *Internet Association Class 25 Comments* at 1 (“[E]xternal security researchers would more readily report any malfunctions, flaws or vulnerabilities to us in order to assist us in improving our offerings – a practice we supports and financially reward through bug bounty programs.”). See also Google, *Chrome Reward Program Rules* (last visited July 31, 2015), <https://www.google.com/about/appsecurity/chrome-rewards/>; PayPal, *PayPal Bug Bounty Program*, (last visited July 31, 2015), <https://www.paypal.com/webapps/mpp/security-tools/reporting-security-issues>.

⁴²⁷ Andrea Matwyshyn noted during the hearing on this proposed class that one researcher “attempted to contact 61 companies with respect to an existing vulnerability. Thirteen had some kind of contact information available.... There was a human-generated response from 28 of these companies out of 61.... And six subsequently released security advisories because of the report.” See *May 26 Hearing Transcript* at 63.

report vulnerabilities, and inadequate internal company resources or processes to address those vulnerabilities in a timely fashion. One researcher, for example, contacted the manufacturer of a device through their generic help desk because that was the only contact information he could find; however, this led to the creation of various help desk tickets and substantial effort until the help desk staff was finally able to inform the appropriate company employee about the vulnerability.⁴²⁸ Other problems arise when an academic notifies the vendor, and the vendor attempts to use the DMCA to keep the academic from publishing results; this creates a conflict with university mandates to publish research.⁴²⁹

Even in the best case scenarios where the vendor ultimately makes the necessary updates to mitigate the vulnerability, researchers sometimes must endure threatening conversations with vendors before their alerts are taken seriously. During the hearings, Mark Stanislav explained the difficulty he experienced trying to track down vendors to notify them of particularly concerning vulnerabilities in a child's Wi-Fi-enabled toy and a home security camera. In these two instances, he stated that the first reactions from the vendor were legal threats rather than substantive discussions regarding the security flaws.⁴³⁰ He noted of these instances:

There are clear examples of how security research not only prevented harm and violations of privacy but also ensured that businesses could continue their business by fixing critical flaws before it impacted their customers adversely. The exemption of security research under the DMCA would remove a large obstacle

⁴²⁸ *Id.* at 155-56.

⁴²⁹ *Id.* at 159 ("One of the issues with notification – and I certainly am in favor of notification. I have done it myself in the times I have found vulnerabilities – is whether or not the vendor would have the legal right to block or delay publication. This actually interacts in a bad way with university policies. I may not accept a grant, for example – this is university policy, not personal policy. I may not accept a grant that gives the funding agency or some outside party the right to block publication. The university sees this as a very fundamental matter of academic freedom that nobody else do it. And it's university policy.").

⁴³⁰ *Id.* at 43-45 ("Upon completion of my research [on the children's toy 'Snort'], I contacted the vendor to explain these issues. Despite my offer to go into details with their engineers, the vendor would not engage with me. Ultimately, my employer at the time received a call from the legal staff of this vendor stating that I must have hacked their company, as that's the only way I could possess this knowledge or have found these vulnerabilities. After a few tense conversations with our respective legal teams, it was determined that the vendor's perception of my actions was not accurate, and productive dialogue finally occurred. These issues were quietly resolved without notifying customers.") ("I found that my own home's web camera that I had been using for quite a while actually had vulnerabilities that could allow a criminal to control full access over the device, including looking at the streaming audio and video of the device that was transmitting from my home... I contacted the vendor to alert them to these issues and offered my assistance to see these issues resolved. The final e-mail I received from their CTO, after going from a range of friendly to threatening, ended up wanting to meet with me to understand how I found these issues as I may have come across confidential information, in their eyes, during this process. Despite my prompt relies, the vendor stopped replying to me and eventually these issues were again quietly resolved without notifying customers.").

for doing what we do best, helping people that are unaware they are in harm's way or helping businesses putting customers in harm's way unintentionally.⁴³¹

Other problems cited in the record include failure by a manufacturer to remedy a flaw, even when the researcher is able to successfully notify the company. One researcher notified a manufacturer of a flaw, and “instead of repairing the system and discussing ways to repair the system, the manufacturer spent considerable resources in an effort to prevent us from publishing the work.”⁴³²

An active, productive discussion is necessary to successfully transform security research into security for users. Vendors may need time to understand a vulnerability, identify affected products and customers, and develop a mitigation strategy. Business practices and the product development life cycle must be factored into the time it may take for vendors to respond. In the case of the recent Stagefright vulnerability, the researchers successfully notified Google of the Android flaw, and Google in turn sent out patches to its partners. However, if manufacturers do not adapt these patches for specific devices, or if carriers do not push these patches out to end user devices, affected devices remain vulnerable.⁴³³ Given the complexities of disclosure, NTIA does not believe that simple, one-size-fits-all standards or best practices in vulnerability disclosure across all sectors and situations are feasible or practical at this time.⁴³⁴

After analyzing the record, and although NTIA strongly supports responsible vulnerability disclosures, NTIA does not recommend that the Librarian attempt to craft a specific disclosure policy to be directly incorporated into a Section 1201 exemption for security research. NTIA recognizes that, in many circumstances, it may be helpful for researchers to collaborate with vendors when they uncover security vulnerabilities. In those cases, NTIA encourages researchers to notify the appropriate vendors of their findings. The issue of disclosure is important and deserves its own debate; however, a rulemaking relating to copyright law is not the appropriate venue to develop disclosure policies. It would be more appropriate for interested parties to, for example, participate in NTIA's multistakeholder process on security vulnerability disclosure to share knowledge of existing standards and practices, and to agree on recommended principles

⁴³¹ *Id.* at 45.

⁴³² *Id.* at 12.

⁴³³ Thomas Fox-Brewster, *Stagefright: It Only Takes One Text to Hack 950 Million Android Phones*, *Forbes*, July 27, 2015, available at <http://www.forbes.com/sites/thomasbrewster/2015/07/27/android-text-attacks/> (“Manufacturers are typically sloth-like in getting patches out to users”).

⁴³⁴ For a bibliography of research, proposed standards, online discussions, and other resources on vulnerability disclosure, see University of Oulu Secure Programming Group, Juhani Eronen & Ari Takanen eds., *Vulnerability Disclosure Publications and Discussion Tracking*, available at https://www.ee.oulu.fi/research/ouspg/Disclosure_tracking.

and approaches around vendor and researcher practices.⁴³⁵ Multiple agencies are examining this particular issue, and policy goals would be better served by their specialized knowledge.⁴³⁶

Therefore, NTIA supports a good faith security exemption for Class 25, which should serve to exempt the security research activities contemplated in Classes 22 and 27 (directed at vehicles and networked medical devices, respectively). NTIA suggests that all requested exemptions for security research be consolidated, and that the Copyright Office recommend one exemption to cover security research generally.⁴³⁷ Finally, where non-copyright interests are at stake, the regulatory agencies with the relevant jurisdictions should address these policy issues. Accordingly, NTIA suggests the following exemption:

⁴³⁵ As part of its broader work on cybersecurity issues, NTIA recently announced that it is convening a multistakeholder process to “develop a broad, shared understanding of the overlapping interests between security researchers and the vendors and owners of products discovered to be vulnerable, and to establish a consensus about voluntary principles to promote better collaboration.” See Multistakeholder Process: Cybersecurity Vulnerabilities, NTIA (Aug. 28, 2015), available at <http://www.ntia.doc.gov/other-publication/2015/multistakeholder-process-cybersecurity-vulnerabilities>. This initiative is unrelated and coincidental to NTIA’s work in this proceeding.

⁴³⁶ See Class 25 Response to Post-Hearing Questions of the Business Software Alliance, June 27, 2015, available at http://copyright.gov/1201/2015/post-hearing/answers/Class_25_Hearing_Response_BSA_Docket_No_2014-07_2015.pdf (noting initiatives from the Department of Commerce Bureau of Industry and Security, The Department of Homeland Security, and pending legislation before the Senate and House of Representatives).

⁴³⁷ NTIA agrees with proponents that distinguishing the classes based on the device the software operates makes little sense, especially considering the limited duration of the exemptions. See Class 25 Comments of the Center for Democracy & Technology, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_StallmanEtAl_Class25.pdf (“Given the rapid proliferation in the kinds of products and systems subject to software-based security flaws and vulnerabilities, an exemption needs to cover more than just a single product or class of product. Product-by-product exemptions—say, for security research regarding the software contained in Internet-connected thermostats—would make little sense in a world where harmful flaws may exist in any of a wide variety of products or systems. Security researches need appropriate legal latitude to engage in good faith security research. If researchers are forced to wait for the next triennial review process each time they discover that software on an additional type of specific product carries significant security vulnerabilities, the damage will already be done. In a world moving at Internet speed, security researchers cannot help protect the public if each new research effort has to be put on hold until the next triennial permission cycle”). Opponents would prefer to keep these exemptions separate from the general security research, as they argue the intricacies of the respective devices created unique concerns. See *GM Class 22 Comments* at 18 (“Cars are not like cell phones or computer programs run on a personal computer. Instead the availability of vehicle software for use at all is contingent upon the continued integrity of vehicle safety systems.”); *Global Automakers Class 22 Comments* at 2 (“The exemption should be denied for the reasons more fully set forth herein, all of which essentially stem from the fact that automotive software is unlike any other copyrighted work subject to such a project exemption”); *AdvaMed Class 25 Comments* at 5 (Unlike the other devices at issues in this proceeding, the “copyrighted medical devices subject to the proposed rulemaking are general not publically available and in most cases are indicated for prescription use or for use by the order of a physician[.]”). These are distinctions without difference—in the context of an analysis of *copyright* law—with respect to the Section 1201 rulemaking. TPMs on software within an ECU in an automobile are not significantly different from the TPMs on software in a desktop computer, and they have the same adverse effects on security research. In addition, software running on various devices often depends on common software libraries, meaning that a vulnerability may exist across multiple device types based on a single, identical software issue (especially as apps move into automobile dashboards). NTIA recognizes that the opponents have concerns tangential to copyright that differ across platforms, but those concerns should be addressed by other relevant regulatory agencies.

Computer programs, in the form of firmware or software, regardless of the device on which they are run, when circumvention is initiated by the owner of the copy of the computer program or with the permission of the owner of the copy of the computer program, in order to conduct good faith security research. This exemption does not obviate the need to comply with other applicable laws and regulations.

H. 3D Printer Software Interoperability with Feedstock (Class 26)

Proponents seek the ability to circumvent technological protection measures on 3D printers (also known as additive manufacturing equipment) to allow use of non-manufacturer-approved feedstock.⁴³⁸ The access controls proponents seek to circumvent vary based on the specific device at issue: In some cases, it is unclear whether one needs to circumvent a TPM that controls access to a copyrighted work,⁴³⁹ while in other cases it appears likely that a copyrighted work is at issue.⁴⁴⁰ To the extent that the prohibition against circumvention applies in this space, an exemption would benefit consumers and the industry by fueling innovation of new feedstocks and reducing costs of feedstock for consumers.⁴⁴¹

Proponents argue that the prohibition against circumvention has a negative impact on their ability to make noninfringing use of works under Section 117 of Title 17, which allows use of copyrighted works to enable machine modification.⁴⁴² Consequently, the prohibition against circumvention has a “significant negative impact on innovation in the 3D printing field, drive[s] up costs for consumers, and undermine[s] expectations of ownership around 3D printers.”⁴⁴³ Proponents identify one brand of proprietary feedstock that costs three times as much as its third-

⁴³⁸ See Class 26 Comments of Public Knowledge and Library Copyright Alliance at 5, Docket No. 2014-07, available at http://copyright.gov/1201/2015/comments-020615/InitialComments_longform_PK_and_LCA_Class26.pdf. NTIA uses the terms “feedstock” and “filament” interchangeably throughout this discussion.

⁴³⁹ One example cited in the record, for example, “relies on a chip verification system in order to force the... printers to only accept filament purchased from 3D Systems.” *Id* at 5.

⁴⁴⁰ For example, “if you’re trying to use a different sort of material [than the standard feedstock supplied by the manufacturer], you might want to change some of the variables in the program itself.” *May 28 Hearing Transcript* at 132.

⁴⁴¹ Class 26 Reply Comments of Public Knowledge at 9-10, Docket No. 2014-07, available at http://copyright.gov/1201/2015/reply-comments-050115/class%2026/ReplyComments_ShortForm_PublicKnowledge_Class26.pdf.

⁴⁴² In the hearing on 3D printing, Sherwin Siy of Public Knowledge explains that “Section 117 allows the making of any copies or adaptations created as an essential step in the utilization of the computer program in conjunction with a machine that’s used in no other manner. So any copies or adaptations that are essential to using that embedded software with that machine” are permitted under copyright law. *May 28 Hearing Transcript* at 144.

⁴⁴³ *PK Class 26 Comments* at 8.

party competitor.⁴⁴⁴ Consumers are further harmed by the inability to use a desired filament in a particular device.⁴⁴⁵ Two commenters further support these claims in stating that third-party filament is sometimes of better quality and less expensive than proprietary feedstock.⁴⁴⁶ Finally, consumer uncertainty regarding the permissibility of circumvention for interoperability of feedstock (uncertainty that does not exist in the market for printer ink cartridges) is stymying third-party feedstock markets.⁴⁴⁷

NTIA is persuaded that an exemption would alleviate these adverse effects. The proposed exemption would encourage experimentation with new feedstocks, reduce costs by stimulating third party filament markets, and reduce uncertainty among those who wish to experiment with their own devices.⁴⁴⁸ On the other hand, NTIA finds the harms identified by the opponents to be unpersuasive. Stratasis argues that granting the exemption would threaten health and safety.⁴⁴⁹ For example, downstream manufacturers might circumvent the TPM on a device and use an inferior, non-manufacturer-approved feedstock material to produce a substandard aircraft part.⁴⁵⁰ NTIA is sensitive to these concerns; however, Section 1201 is a poor fit to ensure quality control in aircraft part manufacturing.⁴⁵¹ As discussed above, NTIA is troubled by the growing misuse of the DMCA to serve non-copyright interests.⁴⁵² Additionally, Stratasis believes that circumvention might otherwise result in harm to its brand.⁴⁵³ Specifically, a consumer might mistakenly criticize the machine rather than the non-proprietary feedstock after producing an

⁴⁴⁴ *Id.* at 9-10 (comparing 3D Systems filament to third party vendors).

⁴⁴⁵ *See May 28 Hearing Transcript* at 179.

⁴⁴⁶ *See Class 26 Combined Comments* at 25, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-020615/EFF_merged_shortform_comments_class26.pdf (Craig Schmidt: “My MakerBot, for example, will not operate properly with MakerBot filament... when using other brands, such as Octave, the printer has run for 20+ hours without jams.”); *id.* at 35 (David Hyland-Wood: “The third party filament is typically cheaper, and often better quality”).

⁴⁴⁷ *See May 28 Hearing Transcript* at 129 (discussing whether *Lexmark* would apply by analogy); *see also PK Class 26 Comments* at 10 (exemption would avoid “wasted years” of innovation).

⁴⁴⁸ *See id.* at 9-10.

⁴⁴⁹ *Class 26 Comments of Stratasis, Ltd.* at 28-29, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/comments-032715/class%2026/STRATASYS_Class26_1201_2014.pdf.

⁴⁵⁰ *See May 28 Hearing Transcript* at 160.

⁴⁵¹ *See id.* at 176 (“[T]he proper enforcement mechanism would be through the revocation of their certification.”); *see also Class 26 Responses to Post-Hearing Questions of Public Knowledge* at 1-2, Docket No. 2014-07, *available at* http://copyright.gov/1201/2015/post-hearing/answers/Class_26_Hearing_Response_Public_Knowledge_Docket_No_2014-07_2015.pdf (conditions would be under inclusive such that it does not prevent unsafe parts, over inclusive such that they would prevent safe uses, and Section 1201 is otherwise unlikely to deter bad actors).

⁴⁵² *See supra* Part I.B – Treatment of Non-Copyright Policy Issues, page 3.

⁴⁵³ *See May 28 Hearing Transcript* at 173.

inferior widget.⁴⁵⁴ NTIA agrees with the proponents that sophisticated users would be the ones utilizing the exemption; therefore, the users would be fully aware that their end-product might differ as a result of using non-manufacturer approved feedstock and would not reflect negatively on the brand of the device.⁴⁵⁵

NTIA supports an exemption that does not distinguish between commercial, noncommercial, or consumer uses of a 3D printer. The advent of 3D printing has caused a blurring of traditional manufacturer-consumer distinctions.⁴⁵⁶ Indeed, opponents of the proposed exemption conceded that such a distinction would be difficult to draw.⁴⁵⁷ For example, manufacturers may use low end or consumer-oriented machines during different parts of the design process.⁴⁵⁸ An exemption that permitted some uses and not others would be problematic to draft, potentially unworkable, and confusing for users.

Similarly, NTIA supports an exemption that permits circumvention of a variety of TPMs in order to use non-manufacturer-approved feedstock. The TPMs implemented on 3D printers vary from manufacturer to manufacturer and may change as technology progresses (*e.g.*, chips on feedstock may become more sophisticated).⁴⁵⁹ A broad exemption that does not distinguish between technical specifications of TPMs would best alleviate the harms identified by the proponents.

NTIA also recognizes that the issues raised in *Lexmark Int'l. Inc. v. Static Control Components, Inc.* have some value in this discussion. An exemption for this class would be consistent with and further the principles identified in *Lexmark*.⁴⁶⁰ In *Lexmark*, the court found that an authentication procedure found in Lexmark toner cartridges constituted a TPM that effectively controlled access to a toner loading program embedded in a printer, but also found

⁴⁵⁴ *Id.* (“If the part comes out not right, it affects our brand, it affects who we are, because they’ll say it’s MakerBot’s junk.”).

⁴⁵⁵ *See id.* at 175.

⁴⁵⁶ *See* Class 26 Response to Post-Hearing Questions of Stratasys, Ltd. (*Stratasys Class 26 Hearing Response*) at 1, June 29, 2015, available at http://copyright.gov/1201/2015/post-Hearing/answers/Class_26_Hearing_Response_Stratasys_Docket_No_2014-07_2015.pdf; *see also* Class 26 Responses to Post-Hearing Questions of Michael Weinberg at 1-2, June 29, 2015, available at http://copyright.gov/1201/2015/post-Hr'g/answers/Class_26_Hearing_Response_Weinberg_Docket_No_2014-07_2015.pdf.

⁴⁵⁷ *See Stratasys Class 26 Hearing Response* at 2 (“Even personal or household uses of a 3D printer may be difficult to classify as ‘noncommercial.’”).

⁴⁵⁸ *See May 28 Hearing Transcript* at 150.

⁴⁵⁹ *See id.* at 185.

⁴⁶⁰ *See Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 549 (6th Cir. 2004) (“In fact, Congress added the interoperability provision in part to ensure that the DMCA would not diminish the benefit to consumers of interoperable devices ‘in the consumer electronics environment.’” The court found that Section 1201 does not cover the circumvention of a technological measure that controls access to a work not protected under Copyright law.).

that the program was not copyrightable.⁴⁶¹ The court also discussed fair use, noting that use of the toner loading program was unlikely to have an adverse market effect on the printer's software. However, because the software was found to be ineligible for copyright protection, a fair use defense was unnecessary.⁴⁶² Still, the holding 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. We therefore support an exemption that reduces the uncertainty in this area and would permit circumvention of TPMs in order to utilize non-manufacturer approved feedstock or filament.

Having analyzed the record, NTIA is persuaded that granting such an exemption is proper, will not adversely affect the market value of copyrighted works, and will provide relief from the harm proponents demonstrated.⁴⁶³ Accordingly, NTIA suggests the following exemption:

Computer programs embedded in 3D printers or similar additive manufacturing devices, as well as in feedstock cartridges used with those devices, where circumvention is undertaken for the purpose of enabling interoperability of feedstock or filament with the device.

⁴⁶¹ *Id.* at 546. The Printer Engine Program was found not to be protected by a TPM, and therefore the DMCA's prohibition against circumvention did not apply. The court also found that the Toner Loader Program was not copyrightable.

⁴⁶² *Id.* at 544-45.

⁴⁶³ *See PK Class 26 Comments* at 8.