LIBRARY OF CONGRESS

U.S. Copyright Office

[Docket No. 2015-8]

Section 1201 Study: Request for Additional Comments

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

ACTION: Notice of Inquiry.

SUMMARY: The United States Copyright Office is requesting additional written comments in connection with its ongoing study on the operation of the statutory provisions regarding the circumvention of copyright protection systems. This request provides an opportunity for interested parties to address certain issues raised by various members of the public in response to the Office's initial Notice of Inquiry.

DATES: Written comments must be received no later than 11:59 p.m. Eastern Time on [INSERT 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. Written reply comments must be received no later than 11:59 p.m. Eastern Time on [INSERT 50 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: The Copyright Office is using the regulations.gov system for the submission and posting of public comments in this proceeding. All comments are therefore to be submitted electronically through regulations.gov. Specific instructions for submitting comments are available on the Copyright Office Web site at *http://copyright.gov/policy/1201/commentsubmission/*. If electronic submission of comments is not feasible, please contact the Office using the contact information below for special instructions.

FOR FURTHER INFORMATION CONTACT: Kevin R. Amer, Senior Counsel for Policy and International Affairs, by email at *kamer@loc.gov* or by telephone at 202-707-8350; or Regan A. Smith, Associate General Counsel, by email at *resm@loc.gov* or by telephone at 202-707-8350.

SUPPLEMENTARY INFORMATION:

I. Background

At the request of the Ranking Member of the House Committee on the Judiciary, the Copyright Office is conducting a study to assess the operation of section 1201 of title 17. In December 2015, the Office issued a Notice of Inquiry identifying several aspects of the statutory and regulatory framework that the Office believes are ripe for review, and inviting public comment on those and any other pertinent issues.[1] The Notice provided for two rounds of written comments. In response, the Office received sixty-eight initial comments and sixteen reply comments.[2] The Office then announced public roundtables on the topics addressed in the Notice and comments.[3] These sessions, held in Washington, D.C. and San Francisco, California in May 2016, involved participation by more than thirty panelists, representing a wide range of interests and perspectives. Transcripts of the roundtables are available at *http://copyright.gov/policy/1201/*, and video recordings will be available at that location at a later date.

In the written comments and during the roundtables, parties expressed a variety of views regarding whether legislative amendments to section 1201 may be warranted.

---

[1] Section 1201 Study: Notice and Request for Public Comment, 80 FR 81369 (Dec. 29, 2015).
[2] All comments may be accessed from the Copyright Office Web site at *http://copyright.gov/policy/1201/* by clicking the "Public Comments" tab, followed by the "Comments" link.
[3] Software-Enabled Consumer Products Study and Section 1201 Study: Announcement of Public Roundtables, 81 FR 17206 (Mar. 28, 2016).

Among other suggested changes, commenters discussed proposals to update the statute's permanent exemption framework and to amend the anti-trafficking provisions to permit third-party assistance with lawful circumvention activities. At this time, as explained below, the Office is interested in receiving additional stakeholder input on particular aspects of those proposals. In addition, parties submitted numerous and varied views regarding the triennial rulemaking process under section 1201(a)(1)(C); while the Office continues to thoroughly evaluate these comments in conducting its study, this second Notice of Inquiry does not specifically address those issues.

A party choosing to respond to this Notice of Inquiry need not address every topic below, but the Office requests that responding parties clearly identify and separately address those subjects for which a response is submitted. Parties also are invited to address any other pertinent issues that the Office should consider in conducting its study.

II. Subjects of Inquiry

1. *Proposals for New Permanent Exemptions*

a. *Assistive Technologies for Use by Persons Who Are Blind, Visually Impaired, or Print Disabled.*

The written comments and roundtable discussions revealed widespread support for adoption of a permanent exemption to facilitate access to works in electronic formats by persons who are blind, visually impaired, or print disabled. The Office invites comment regarding specific provisions that commenters believe should be included in legislation proposing such an exemption. For example, the exemption for this purpose granted in the 2015 rulemaking permits circumvention of access controls applied to literary works distributed electronically, where the access controls "either prevent the

enabling of read-aloud functionality or interfere with screen readers or other applications or assistive technologies."[4] The exemption applies in the following circumstances:

> (i) When a copy of such a work is lawfully obtained by a blind or other person with a disability, as such a person is defined in 17 U.S.C. 121; provided, however, that the rights owner is remunerated, as appropriate, for the price of the mainstream copy of the work as made available to the general public through customary channels, or
>
> (ii) When such work is a nondramatic literary work, lawfully obtained and used by an authorized entity pursuant to 17 U.S.C. 121.[5]

The Office is interested in commenters' views on whether this language would be appropriate for adoption as a permanent exemption, or whether there are specific changes or additional provisions that Congress may wish to consider.

b. *Device Unlocking.* Some commenters advocated the adoption of a permanent exemption to permit circumvention of access controls on wireless devices for purposes of "unlocking" such devices—*i.e.*, enabling them to connect to the network of a different mobile wireless carrier. Since 2006, the rulemaking process has involved consideration of exemptions permitting unlocking of cellphones, and in the 2015 rulemaking, pursuant to Congress's direction,[6] the Register considered whether to extend the exemption to other categories of wireless devices. At the conclusion of the 2015 proceeding, the Librarian, upon the Register's recommendation, adopted an unlocking exemption that applies to used wireless devices of the following types:

(A) Wireless telephone handsets (*i.e.*, cellphones);

(B) All-purpose tablet computers;

---

[4] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 FR 65944, 65950 (Oct. 28, 2015) ("2015 Final Rule").
[5] *Id.*
[6] *See* Unlocking Consumer Choice and Wireless Competition Act, Pub. L. No. 113–144, sec. 2(b), 128 Stat. 1751, 1751 (2014).

(C) Portable mobile connectivity devices, such as mobile hotspots, removable wireless broadband modems, and similar devices; and

(D) Wearable wireless devices designed to be worn on the body, such as smartwatches or fitness devices.[7]

The Office invites comment on whether an unlocking exemption would be appropriate for adoption as a permanent exemption or whether such activities are more properly considered as part of the triennial rulemaking. For commenters who favor consideration of a permanent exemption, the Office is interested in commenters' views on whether the language of the 2015 unlocking exemption would be appropriate for adoption as a permanent exemption, or whether there are specific changes or additional provisions that Congress may wish to consider.

c. *Computer Programs.* Several commenters expressed concern over the scope of section 1201 in the context of copyrighted computer programs that enable the operation of a machine or device. These commenters suggested that by prohibiting the circumvention of access controls on such programs, the statute prevents the public from engaging in legitimate activities, such as the repair of automobiles or the use of third-party device components, that seem far removed from the protection of creative expression that section 1201 was intended to address. To respond to this concern, some commenters argued that Congress should establish a statutory exemption that would permit circumvention of technological protection measures ("TPM"s) controlling access to such software in appropriate circumstances. The Office is interested in additional views on such proposals.

[7] 2015 Final Rule, 80 FR at 65952.

For purposes of focusing the discussion, the Office invites comment on whether there are specific formulations of such an exemption that could serve as helpful starting points for further consideration of legislation. For example, Congress could consider adoption of a permanent exemption for purposes of diagnosis, maintenance, and repair. Such legislation could provide that a person who has lawfully obtained the right to use a computer program may circumvent a TPM controlling access to that program, so long as the circumvention is undertaken for purposes of diagnosis, maintenance, or repair. Are existing legal doctrines or statutes, such as the current language addressing machine maintenance and repair in section 117(c),[8] the doctrine of repair and reconstruction in patent law,[9] case law addressing refurbishment under trademark law,[10] or "right to repair" bills introduced into various state legislatures,[11] helpful to inform the appropriate scope of repair in this context? To what extent would the combination of such an exemption with the current language of 1201(f)[12]—which allows circumvention for purposes of facilitating interoperability under certain circumstances—adequately address users' concerns regarding section 1201's impact on consumer activities?

Please also comment upon whether it would be advisable to consider, in addition to diagnosis, maintenance, or repair, an exemption to explicitly permit circumvention for

[8] 17 U.S.C. 117(c).
[9] *See Aro Mfg. Co. v. Convertible Top Replacement Co*., 365 U.S. 336 (1961); *see also Aro Mfg. Co. v. Convertible Top Replacement Co*., 377 U.S. 476 (1964).
[10] *See Champion Spark Plug Co. v. Sanders*, 331 U.S. 125 (1947); *see also Karl Storz Endoscopy-America, Inc. v. Fiber Tech Med., Inc.*, 4 F. App'x 128, 131-32 (4th Cir. 2001) ("[T]he Lanham Act does not apply in the narrow category of cases where a trademarked product is repaired, rebuilt or modified at the request of the product's owner," so long as "the owner is not, to the repairer's knowledge, merely obtaining modifications or repairs for purposes of resale.").
[11] *See, e.g.*, H.R. 3383, 189th Gen. Ct. (Mass. 2015); S. 3998B, 2015 Leg., Reg. Sess. (N.Y. 2015); Assemb. 6068A, 2015 Leg., Reg. Sess. (N.Y. 2015); Legis. B. 1072, 104th Leg., 2d Sess. (Neb. 2016); H.R. 1048, 89th Leg., Reg. Sess. (Minn. 2015); *see also* MASS. GEN. LAWS ch. 93K (2013).
[12] 17 U.S.C. 1201(f).

purposes of engaging in any lawful modification of a computer program. Such an exemption could allow circumventions undertaken to make non-infringing adaptations, including, for example, uses permitted under section 117(a) and/or the fair use doctrine.[13] Please address whether this broader formulation would, or would not, be likely to result in economically harmful unauthorized uses of copyrighted works.

With either formulation, would concerns over enabling unauthorized uses be mitigated by conditioning the exemption on the circumventing party not engaging in any unauthorized use of a copyrighted work other than the accessed computer program, or by limiting the exemption to computer programs that are "not a conduit to protectable expression"—*i.e.*, those that do "not in turn create any protected expression" when executed?[14] In the United Kingdom, for example, the prohibition on circumvention specifically excludes TPMs applied to computer programs, but does apply in at least some circumstances where copyrighted content is generated by a computer program (*e.g.*, graphical content in video games).[15] The Office is particularly interested in any information or perspectives on the impact of the UK law and how operating under it contrasts or not with the U.S. experience. Alternatively, should the exemption be limited to computer programs in particular categories of devices?

The Office is interested in commenters' views on the advisability of these various approaches. Which of these models, if any, would facilitate users' ability to engage in permissible uses of software, while preserving congressional intent in supporting new

[13] *See* 17 U.S.C. 117(a), 107.
[14] *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 548 (6th Cir. 2004).
[15] Copyright, Designs and Patents Act 1988, c. 48, § 296ZA (UK); *see Nintendo Co. Ltd. v. Playables Ltd.* [2010] EWHC 1932 (Ch) (Eng.) (construing related anti-trafficking provision).

ways of disseminating copyrighted materials to users?[16] Responding parties are also encouraged to suggest alternate formulations, keeping in mind the Office's goal of focusing discussion on this topic.

d. *Obsolete Technologies.* In prior rulemakings, the Copyright Office and the Librarian of Congress have considered multiple petitions to permit circumvention of an access control mechanism protecting a given class of works that fails to permit access because of malfunction, damage, or obsoleteness.[17] The Office has recommended, and the Librarian has adopted, multiple exemptions after finding that the definition of "obsolete" in section 108 captures the circumstances under which such an exemption was justified, *i.e.*, where the access control "is no longer manufactured or is no longer reasonably available in the commercial marketplace."[18] The Office is interested in commenters' views on whether Congress should consider a legislative amendment to permit circumvention of such faulty access controls, or whether there are other specific changes or additional provisions that Congress may wish to consider to address this issue.

---

[16] *See* STAFF OF H. COMM. ON THE JUDICIARY, 105TH CONG., SECTION-BY-SECTION ANALYSIS OF H.R. 2281 AS PASSED BY THE UNITED STATES HOUSE OF REPRESENTATIVES ON AUGUST 4TH, 1998, at 6 (Comm. Print 1998).

[17] *See, e.g.*, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 FR 64556, 64564–66, 64574 (Oct. 27, 2000) ("2000 Recommendation and Final Rule"); Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Final Rule, 68 FR 62011, 62013–16 (Oct. 31, 2003) ("2003 Final Rule"); Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 FR 68472, 68474–75, 68480 (Nov. 27, 2006) ("2006 Final Rule"); Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 75 FR 43825, 43833–34, 43839 (July 27, 2010) ("2010 Final Rule"); 2015 Final Rule, 80 FR at 65955, 65961.

[18] 17 U.S.C. 108(c); *see, e.g.*, 2000 Recommendation and Final Rule, 65 FR at 64565–66; Recommendation of the Register of Copyrights in RM 2002-4; Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies 40 (Oct. 27, 2003); 2003 Final Rule, 68 FR at 62013–14; Recommendation of the Register of Copyrights in RM 2005-11; Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies 36 & n.105 (Nov. 17, 2006); 2006 Final Rule, 71 FR at 68475.

e. *International Considerations.* In addition to the questions on specific proposals provided above, please discuss the interaction of these proposals with existing international obligations of the United States, including free trade agreements.

2. *Proposed Amendments to Existing Permanent Exemptions*

Some parties expressed the view that the existing permanent exemptions for security testing, encryption research, and reverse engineering[19] do not adequately accommodate good-faith research into malfunctions, security flaws, and vulnerabilities in computer programs.[20] The Office invites comment on whether legislation to address this concern may be warranted, and if so, on specific changes that should be considered. In particular, the Office requests commenters' views on the following topics:

a. In the 2015 rulemaking, the Register recommended, and the Librarian of Congress adopted, an exemption that permits circumvention of TPMs controlling access to computer programs in the following circumstances:

> (i) . . . the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates solely for the purpose of good-faith security research and does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986, as amended and codified in title 18, United States Code; . . . and the device or machine is one of the following:
>
> (A) A device or machine primarily designed for use by individual consumers (including voting machines);
>
> (B) A motorized land vehicle; or
>
> (C) A medical device designed for whole or partial implantation in patients or a corresponding personal monitoring system, that is not and

[19] 17 U.S.C. 1201(f), (g), (j).

[20] Similarly, in the 2015 rulemaking, the Register noted that section 1201(j) "does not seem sufficiently robust in light of the perils of today's connected world." U.S. Copyright Office, Section 1201 Rulemaking: Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention 3(2015), http://copyright.gov/1201/2015/registersrecommendation.pdf ("2015 Recommendation").

will not be used by patients or for patient care.

> (ii) For purposes of this exemption, "good-faith security research" means accessing a computer program solely for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability, where such activity is carried out in a controlled environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement.[21]

The Office is interested in commenters' views on whether this language would be appropriate for adoption as a permanent exemption, or whether there are specific changes or additional provisions that Congress may wish to consider.

b. The exemption for security testing under section 1201(j) is limited to activities undertaken "with the authorization of the owner or operator of [the] computer, computer system, or computer network."[22] In the 2015 rulemaking, the Register noted that in some cases "it may be difficult to identify the relevant owner" for purposes of this requirement and that "it may not be feasible to obtain authorization even where there is an identifiable owner."[23] Echoing those concerns, one group of commenters argued that the authorization requirement should be eliminated, while another urged Congress to provide greater clarity in situations involving multiple owners. Please assess whether legislation may be appropriate in this area and discuss any specific legislative proposals that you believe should be considered.

[21] 2015 Recommendation at 319-20; 2015 Final Rule, 80 FR at 65956.
[22] 17 U.S.C. 1201(j)(1).
[23] 2015 Recommendation at 309.

c. Section 1201(j) provides a two-factor framework to determine whether a person qualifies for the security testing exemption.[24] In the 2015 rulemaking, the Register noted that these factors "would appear to be of uncertain application to at least some" security research activities.[25] Some commenters advocated the removal of one or both of these factors from the statute.[26] Please assess the advisability of such changes, or discuss any other specific legislative proposals you believe should be considered.

d. The exemption for encryption research in section 1201(g) is similarly limited to activities qualifying under a four-factor framework that includes making "a good faith effort to obtain authorization" before the circumvention.[27] In the 2015 rulemaking, the Register noted that meeting these requirements "may not always be feasible" for researchers.[28] Please assess whether legislation may be appropriate in this area and discuss any specific legislative proposals that you believe should be considered.

e. Section 1201(f) permits circumvention for the "sole purpose" of identifying and analyzing elements of computer programs necessary to achieve interoperability.[29] In the 2015 rulemaking, the Register noted that "section 1201(f)(1) is limited to circumvention solely for the identification and analysis of program elements necessary for interoperability, and does not address circumvention after that analysis has

[24] 17 U.S.C. 1201(j)(3).
[25] 2015 Recommendation at 309.
[26] The proposed Breaking Down Barriers to Innovation Act of 2015 would eliminate the two-factor framework, as well as the multifactor framework under section 1201(g)(3). H.R. 1883, 114th Cong. sec. 3(c)(3), 3(e)(2) (2015); S. 990, 114th Cong. sec. 3(c)(3), 3(e)(2) (2015).
[27] 17 U.S.C. 1201(g)(2)(C).
[28] 2015 Recommendation at 307.
[29] 17 U.S.C. 1201(f).

been performed."[30] Please assess whether legislation may be appropriate in this area and discuss any specific legislative proposals that you believe should be considered.

3. *Anti-Trafficking Provisions*

Commenters offered differing views regarding the role of the anti-trafficking provisions under sections 1201(a)(2) and 1201(b). User groups expressed concern that, to the extent these provisions prohibit third parties from providing assistance to beneficiaries of exemptions, or prohibit the making and distribution of necessary tools, they undermine beneficiaries' practical ability to engage in the permitted conduct. Copyright owners, however, cautioned against amendment of the anti-trafficking provisions, arguing that because circumvention tools may be used for lawful and unlawful purposes alike, it would be impossible to ensure that tools manufactured and distributed pursuant to an exemption, once available in the marketplace, would be employed solely for authorized uses. The Office is interested in receiving additional views on this topic, and specifically invites comment on the following issues:

a. A few parties argued that section 1201 contains an implied right permitting a beneficiary of a statutory or administrative exemption to make a tool for his or her own use in engaging in the permitted circumvention. What are commenters' views regarding this interpretation of the statute? To what extent, if any, does the statutory prohibition on the "manufacture" of circumvention tools affect the analysis?[31] If such a right is not currently implied, or the question is uncertain, should Congress consider amending the statute to expressly permit such activity, while maintaining the prohibition against trafficking in such tools?

[30] 2015 Recommendation at 337 n.2295.
[31] *See* 17 U.S.C. 1201(a)(2), (b)(1).

b. Some parties suggested that, in certain circumstances, third-party assistance may fall outside the scope of the anti-trafficking provisions and therefore may be permissible under current law. What are commenters' views regarding this interpretation of the statute? Are there forms of third-party assistance that do not qualify as a "service" within the meaning of sections 1201(a)(2) and 1201(b)(1)? If so, what considerations are relevant to this analysis?

Dated: September 21, 2016.

_____

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

[BILLING CODE 1410-30-P]

[FR Doc. 2016-23167 Filed: 9/26/2016 8:45 am; Publication Date: 9/27/2016]