Submission on behalf of Joint Creators and Copyright Owners
Class 13: Computer Programs – Security Research

UNITED STATES COPYRIGHT OFFICE

Long Comment Regarding a Proposed Exemption Under 17 U.S.C. § 1201

[ ] Check here if multimedia evidence is being provided in connection with this comment

ITEM A. COMMENTER INFORMATION

The Motion Picture Association, Inc. ("MPA") is a trade association representing some of the world's largest producers and distributors of motion pictures and other audiovisual entertainment for viewing in theaters, on prerecorded media, over broadcast TV, cable and satellite services, and on the internet. The MPA's members are: Netflix Studios, LLC, Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Universal City Studios LLC, Walt Disney Studios Motion Pictures, and Warner Bros. Entertainment Inc.

The Alliance for Recorded Music ("ARM") is a nonprofit coalition comprising the many artists and record labels who together perform, create, and/or distribute nearly all of the sound recordings commercially released in the United States. Members include the American Association of Independent Music ("A2IM"), the Music Artists Coalition ("MAC"), the Recording Industry Association of America, Inc. ("RIAA"), hundreds of recording artists, the major record companies, and more than 600 independently owned U.S. music labels.

The Entertainment Software Association ("ESA") is the United States trade association serving companies that publish computer and video games for video game consoles, handheld video game devices, personal computers, and the internet. It represents nearly all of the major video game publishers and major video game platform providers in the United States.

Represented By:
J. Matthew Williams (mxw@msk.com)
Sofia Castillo (szc@msk.com)
MITCHELL SILBERBERG & KNUPP LLP
1818 N Street, NW, 7th Floor
Washington, D.C. 20036
202-355-7904

ITEM B. PROPOSED CLASS ADDRESSED

Proposed Class 13: Computer Programs — Security Research

ITEM C. OVERVIEW

Legitimate security research is an important practice. Many companies participate in the security testing ecosystem by cooperating with good-faith researchers. As such, MPA, ARM and ESA

("Joint Creators and Copyright Owners") did not oppose continuation of the existing security testing exemption, which the Copyright Office has already recommended for renewal. The existing regulatory exemption, in addition to Congress's statutory exception for security testing codified in Section 1201(j), already provide the shields from liability that legitimate researchers need to circumvent access controls to conduct security testing. Similarly, Section 1201(i) may provide the necessary liability shield for privacy researchers.

The Copyright Office carefully crafted the language in the current exemption to balance the needs of legitimate researchers with the protection of not only copyrighted works, but also of the public's well-being. The Copyright Office's prior recommendation that the "Librarian exercise a degree of caution in adopting an exemption" in this arena exemplifies the importance of containing the scope of the exemption.[1]

Nevertheless, proponents Professor J. Alex Halderman, Center for Democracy & Technology, and U.S. Technology Policy Committee of the Association for Computing Machinery ("Halderman"), with the support of HackerOne, Inc., Free Software Foundation, and Rapid7, seek to delete nearly every limitation from the existing exemption. They attempt to justify doing so by presenting almost exactly the same arguments that were presented in prior cycles and during the process that resulted in the June 2017 Section 1201 Study, where the Copyright Office proposed that Congress utilize the current exemption as a "starting point" for drafting any new statutory exception related to security research.[2]

In sum, these Petitioners' proposal lacks sufficient justification for removal of the necessary limitations specified in the current exemption. Each of the limitations in the current exemption should be maintained.

We also question Software Freedom Conservancy, Inc.'s ("SFC") proposal to expand the existing security research exemption to permit consumers to "remove software or disable functionality that may expose personal information."[3] As discussed below, the need for the exemption and its proposed scope are doubtful.

ITEM D. TECHNOLOGICAL PROTECTION MEASURE(S) AND METHOD(S) OF CIRCUMVENTION

Halderman's proposed expanded exemption would cover TPMs in a variety of devices, including challenge response measures (such as access codes, passwords, keys, and digital signatures), encryption, and software designed to prevent tampering, or software that controls

---

[1] SECTION 1201 RULEMAKING: SIXTH TRIENNIAL PROCEEDING TO DETERMINE EXEMPTIONS TO THE PROHIBITION ON CIRCUMVENTION, RECOMMENDATION OF THE REGISTER OF COPYRIGHTS 317 (2015), https://www.copyright.gov/1201/2015/registers-recommendation.pdf ("2015 Rec.").

[2] *See id*. at 306, 312–18; U.S. COPYRIGHT OFFICE, SECTION 1201 OF TITLE 17 71-80 (2017), https://www.copyright.gov/policy/1201/section-1201-full-report.pdf ("1201 Study").

[3] SFC, Class 13 Long Comment at 2 (Dec. 14, 2020), https://www.copyright.gov/1201/2021/comments/Class%2013_Initial%20Comment_Software%20Freedom%20Conservancy.pdf ("SFC 2020 Comment").

installation, execution, use, reading or inspection, or modification.[4] The universe of access controls at issue is impossible to address with any specificity.

That is also true of SFC's proposal, which seeks to cover "installing legitimately obtained software on devices for the purpose of evaluating the device's functionality, de-obfuscating and decompiling code in order to study it, and accessing protected memory spaces to evaluate the software within."[5]

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

> The current regulation exempts circumvention to access:
>
> (i) Computer programs, where the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates, or is undertaken on a computer, computer system, or computer network on which the computer program operates with the authorization of the owner or operator of such computer, computer system, or computer network, 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. (ii) For purposes of this paragraph (b)(11), "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 an 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.[6]

1. The Record Does not Justify the Elimination of Common-Sense Limitations in the Existing Exemption for Security Research

Halderman seeks to expand the existing exemption (which was recommended for renewal) to remove the limitations on purpose, security, lawful acquisition, and violating other laws.[7] As discussed below, these "limitations" are common-sense ways of tailoring the exemption to attempt to cover only legitimate conduct. As in prior cycles, the limitations should all be retained.

---

[4] *See* Halderman *et al*., Class 13 Long Comment at 11-12 (Dec. 14, 2020), https://www.copyright.gov/1201/2021/comments/Class%2013_InitialComments_J.%20Alex%20Halderman,%20Center%20for%20Democracy%20&%20Technology,%20and%20U.S.%20Technology%20Policy%20Committee%20of%20the%20Association%20for%20Computing%20Machinery.pdf ("Halderman 2020 Comment").

[5] SFC 2020 Comment at 3.

[6] 37 C.F.R. § 201.40(b) (11).

[7] Halderman 2020 Comment at 5. Petitioners appear to use the word "limitation" in a pejorative fashion. However, every exemption should contain proper limitations.

(a) The "Purpose" and "Security" Limitations

The exemption rightfully cabins its scope to ensure circumvention is accomplished "solely" for the purpose of accessing software to conduct good-faith testing, investigation, and correction of flaws or vulnerabilities. This was based on language used by Congress in multiple instances in Section 1201. There is no evidence indicating this language exposes researchers to malicious litigation when they seek to study, develop solutions to, or inform the public about dangerous vulnerabilities in software, to engage in scientific dialogue or implement protective measures, or engage in academic peer review, classroom teaching, or to publish updates to the security community.[8] The Copyright Office has correctly attempted to ensure that security research cannot become a back door to enable unauthorized access to works and other harmful acts. In fact, that is the very task that Congress assigned to the Copyright Office.

In its 2018 Recommendation, the Copyright Office rejected Halderman's request to eliminate this limitation because it "is not properly read to prohibit teaching, academic dialogue, or scholarship involving information derived from good-faith security research."[9] It further explained that this limitation is unlikely to have an adverse effect because it focuses on:

> the researcher's purpose at the time of circumvention. While post-circumvention activities might be relevant to the extent they provide evidence on that issue, a researcher who at the time of circumvention intends to publish the results of good-faith research or use them in the course of teaching would not exceed the bounds of the Access Limitation. Such activities ordinarily are expected to follow from research, and therefore they easily fit within the meaning of the regulatory language when read in its proper context.[10]

The exemption also rightfully requires that the research be "primarily to promote the security or safety of the class of devices or machines" at issue.[11] Halderman's claim that "primarily" could be read as "only" is specious and misguided.[12] The Copyright Office also rejected this argument in 2018 because "it is not plausible to conclude that the term 'primarily' could be interpreted to mean 'only.' Those two terms clearly are not synonymous, and nothing in the record suggests that any copyright holder has advanced such a reading."[13]

---

[8] *Id.* at 18, 21. Petitioners' description of the takedown notice sent by RIAA to GitHub, and the circumstances of that notice, is inaccurate. It is also inapposite, as even they admit that the "incident did not involve security research." *Id.* at 21-22.

[9] SECTION 1201 RULEMAKING: SEVENTH TRIENNIAL PROCEEDING TO DETERMINE EXEMPTIONS TO THE PROHIBITION ON CIRCUMVENTION: RECOMMENDATION OF THE ACTING REGISTER OF COPYRIGHTS 305 (2018), https://cdn.loc.gov/copyright/1201/2018/2018_Section_1201_Acting_Registers_Recommendation.pdf ("2018 Rec.").

[10] *Id.* at 305-06.

[11] 37 C.F.R. § 201.40(b) (11) (ii).

[12] Halderman 2020 Comment at 21.

[13] 2018 Rec. at 309.

Halderman claims (again) that the language is too ambiguous, thereby limiting researchers' speech.[14] If the commenters desire more clearly defined rules on what may be done with the results of the research, then the Copyright Office should consider including express guidelines in the exemption regarding how research results are disseminated. For example, notifying the distributor of the software and/or device at issue of the flaw and providing reasonable time to correct the issue before publishing the results is a reasonable and preferable practice. Although the Copyright Office previously concluded that "determining the relevant 'developer' to whom information must be disclosed could be difficult if not impossible in some instances," that potentiality should not prevent the Copyright Office from requiring researchers to at least attempt to identify the developer, distributor, or publisher and provide an opportunity for flaw correction.[15]

Finally, the exemption disallows the facilitation of copyright infringement. The revised language proposed by Halderman fails to preserve this limitation on the scope of the exemption. Preserving such limitation is critically important, as it is in connection with other exemptions.

(b) The "Lawfully Acquired" Limitation

Halderman asks the Copyright Office to recommend the removal of the requirement that the device researched be "lawfully acquired" because "where researchers acquire a device in a legitimate manner, they nevertheless cannot be certain whether they will still qualify for the exemption because the legality of acquisition is often dependent on the actions of third parties over which researchers have no knowledge or control."[16] In 2018, the Copyright Office rejected an identical request due to the absence in the record of any indication of this type of dispute and "and speculation alone is insufficient to demonstrate a likely adverse effect."[17] The Copyright Office also concluded that the phrase "lawfully acquired" is not ambiguous and "does not require that the circumventing party be the lawful owner of the device—or the software embedded within the device—only that the device be lawfully acquired."[18]

The Copyright Office should arrive at the same conclusion in this cycle. As in 2018, there is no indication in Halderman's 2020 petition that any disputes of the type described by proponents have materialized. Moreover, the Copyright Office should not alter the current exemption; it aligns with the common sense approach that Congress itself adopted in the Copyright Act.[19]

---

[14] Halderman 2020 Comment at 18, 21.

[15] 2015 Rec. at 309.

[16] Halderman 2020 Comment at 23.

[17] 2018 Rec. at 303.

[18] *Id.*

[19] *See* H.R. Rep. No. 105-796, 105th Cong. 2d Sess., at 67 (Oct. 8, 1998) ("[T]he scope of permissible security testing under the Act should be the same as permissible testing of a simple door lock: a prospective buyer may test the lock at the store with the store's consent, or may purchase the lock and test it at home in any manner that he or she sees fit. . . . What that person may not do, however, is test the lock once it has been installed on someone else's door, without the consent of the person whose property is protected by the lock.").

(c) The "Any Laws" Limitation

Halderman suggests that the Copyright Office should discard the requirement that circumvention must "not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986."[20] In 2017, in connection with the Section 1201 Study, the Copyright Office stated that "it was not clear . . . that the requirement to comply with other laws impedes legitimate security research [, as] other laws still apply even if the activity is permitted under section 1201."[21] The Copyright Office accordingly did not recommend any legislative reform on this point. This approach to resolving this issue remains valid based on the record in this proceeding.

Halderman claims that this language creates uncertainty "by making the entire body of federal, state, and local law a trigger for liability under Section 1201."[22] This is a red herring. Congress wrote a similar requirement that researchers must comply with laws other than the Copyright Act into the statutory security testing exemption, Section 1201(j). Thus, Congress clearly had no problem with other laws being considered in connection with Section 1201, and neither should the Copyright Office. Moreover, under 17 U.S.C. § 1204(a), the research would have to be willfully in violation of Section 1201 and for the purpose of commercial advantage or private financial gain, to trigger criminal liability. Also, educational institutions are exempt from criminal liability under 17 U.S.C. § 1204(b). Thus, Section 1201 already has built-in boundaries that address the commenters' concerns.

2. The Record Raises Questions Concerning Expanding the Current Exemption to Include Privacy Research and Related Modification of Code/Devices

SFC seeks the expansion of the existing security research exemption to permit "good-faith testing, investigation, and/or correction of privacy issues (including flaws or functionality that may expose personal information) and permits the owner of the device to remove software or disable functionality that may expose personal information."[23]

SFC contends that this expansion is necessary because privacy research does not always overlap with security research, which means the current exemption would not protect all privacy research activities that may require circumvention.[24] For example, SFC states that privacy research is sometimes unrelated to security issues, and instead focuses on the collection of data in excess of

[20] *Id.* at 5.

[21] 1201 Study at 80.

[22] Halderman 2020 Comment at 23.

[23] SFC 2020 Comment at 2. SFC also makes passing mention of removing or altering hardware, but the need to do so is unclear from the comments. *Id.* at 4. In the past, the Copyright Office has treated hardware and software distinctly.

[24] *Id.* at 2.

disclosed privacy policies. Whether this position has merit is unclear from prior rulemaking records, where privacy issues have been discussed.[25]

SFC also claims that the permanent exemption on privacy in Section 1201(i) is inadequate because it purportedly only covers end users, rather than privacy researchers.[26] However, in order to research code on a device and its associated privacy practices, a researcher must use the device in some manner. So this interpretation of the provision is questionable. SFC also points out that Section 1201(i) is limited to the collection of information concerning "online activities," while some devices may collect information concerning offline activities.[27] But presumably that is accomplished through the online connectivity of devices, so this distinction is also questionable.

While protecting legitimate privacy interests is an important practice, the Joint Creators and Copyright Owners have questions concerning the scope of SFC's proposal. For example:

- If the objective is to identify data collection practices that are inconsistent with announced privacy policies, would the proposal allow for altering code/devices that are in compliance with such policies? The comments imply that it would.[28]

- If a consumer has access to works, including via subscription services, conditioned on articulated data collection practices, would the proposal allow for altering code/devices in a manner inconsistent with the terms and conditions of use? If so, the conduct may be infringing in some circumstances.

- What is the scope of the covered computer programs? SFC appears to focus on embedded device software, rather than on websites, networks, or online databases.[29]

We also reiterate that the limitations on the existing security research exemption should be maintained if any expanded or new exemption is granted for privacy research.

[25] Privacy issues have not only been discussed in connection with security research, but also in connection with jailbreaking exemptions.

[26] SFC 2020 Comment at 2.

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

[28] *Id.* at 11.

[29] SFC does make reference to "modifications to networking equipment." *Id.* at 10.

F. DOCUMENTARY EVIDENCE

We have included hyperlinks to webpages/documents within the body of this document. We are not submitting any other documentary evidence.

Respectfully submitted:

/s/ J. Matthew Williams
J. Matthew Williams (mxw@msk.com)
Sofia Castillo (szc@msk.com)
MITCHELL SILBERBERG & KNUPP LLP
1818 N Street, NW, 7th Floor
Washington, D.C. 20036
202-355-7904