This is a Word document that allows users to type into the spaces below. The comment may be single-spaced, but should be in at least 12-point type. The italicized instructions on this template may be deleted.

UNITED STATES COPYRIGHT OFFICE

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

Please submit a separate comment for each proposed class.

NOTE: This form must be used in all three rounds of comments by all commenters not submitting short-form comments directly through regulations.gov, whether the commenter is supporting, opposing, or merely providing pertinent information about a proposed exemption.

When commenting on a proposed expansion to an existing exemption, you should focus your comments only on those issues relevant to the proposed expansion.

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

Commenters can provide relevant multimedia evidence to support their arguments. Please note that such evidence must be separately submitted in conformity with the Office's instructions for submitting multimedia evidence, available on the Copyright Office website at https://www.copyright.gov/1201/2021.

ITEM A. COMMENTER INFORMATION

Christian Troncoso (christiant@bsa.org) on behalf of BSA | The Software Alliance ("BSA").

BSA is the leading advocate for the global software industry before governments and in the international marketplace. It is an association of world-class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life. BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, CNC/Mastercam, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

ITEM B. PROPOSED CLASS ADDRESSED

Proposed Class 13: Computer Programs – Security Research

ITEM C. OVERVIEW

As businesses that rely on consumer trust, BSA members understand the importance of ensuring the security of their products and services. At every stage of the software development lifecycle, from design to deployment, BSA members invest substantial resources into securing their products. In addition to maintaining their own security teams, BSA members also actively cooperate with the independent security research community to identify potential vulnerabilities and prevent their exploitation.

BSA members agree that the DMCA should not impede good-faith security research. Recognizing the importance of such research to the security of the software system ecosystem, BSA has for consecutive rulemaking cycles strongly supported renewal of a security research exemption. The security research exemption granted by the Librarian of Congress during the 2018 rulemaking cycle and reflected in 37 C.F.R. § 201.40(b)(11) (hereinafter "2018 Exemption"), reflects a careful balance that accommodates the needs of the independent security research community, the property interests of copyright owners, Congressional intent about the scope of "good-faith security research" reflected in § 1201(j), and the significant public safety risks that could be implicated by an overly-broad exemption. To balance these interests, the 2018 Exemption includes a number of critical security safeguards:

1. **Purpose Limitation:** The 2018 Exemption is limited to circumvention carried out "solely for the purpose of good-faith security research," which is defined as "accessing a computer program solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability."
2. **Security/Use Limitation:** The 2018 Exemption is limited to ensure that "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
3. **Lawfully Acquired Limitation:** The 2018 Exemption is limited to circumvention "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."
4. **Any Laws Limitation:** The 2018 Exemption is limited to circumvention activity that "does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act."

The petition submitted by Professor J. Alex Halderman, the Center for Democracy and Technology, and the U.S. Technology Policy Committee of the Association for Computing Machinery (hereinafter "Petitioners") seeks to eliminate *all* of these critical safeguards. In support of their request, Petitioners argue that the safeguards adversely affect their ability to engage in certain forms of non-infringing security research. Notably, the arguments raised by Petitioners are virtually identical to those raised in the context of the 2018

Rulemaking. During that rulemaking, the Acting Register of Copyrights determined that each of the adverse effects cited by Petitioners derived from either an unreasonable interpretation of the limitations or were necessary to adhere to Congressional intent and the DMCA's limited grant of authority to the Librarian of Congress under § 1201(a)(1). Because Petitioners assert no material change in law, fact or circumstance since the 2018 Rulemaking to warrant the removal of these important limitations, the Register should again decline the invitation to remove the safeguards.

In a separate petition, the Software Freedom Conservancy has proposed expanding the definition of "good-faith security research" so that it also includes "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." The Software Freedom Conservancy explains that the existing statutory exception that governs circumvention related to privacy – § 1201(i) – is too narrow to accommodate the needs of the independent privacy research community. Given the existence of this separate statutory analogue, it would be inappropriate to expand the security research exemption – which has its own statutory analogue in § 1201(j) – to address the privacy-related concerns raised by the Software Freedom Conservancy. The security research exemption reflected in 37 C.F.R. § 201.40(b)(11) incorporates a number of considerations and safeguards that reflect an effort to address the needs of the security research community in a manner that adheres to the underlying Congressional intent reflected § 1201(j). To the extent a privacy research exemption is deemed warranted, it should likewise incorporate some of the key safeguards from § 1201(i).

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

[Intentionally left blank]

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

1. Purpose Limitation

The Purpose Limitation provides that circumvention is permitted when undertaken "solely for the purpose of good-faith security research," which is defined as "accessing a computer program solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability." Petitioners contend that the Purpose Limitation "deprives researchers of sufficient clarity about whether the exemption permits engaging in scholarship or criticism related to copyrighted materials protected by a TPM."[1] The Copyright Office considered a similar argument during the 2018

[1] Halderman, CDT, ACM Petition at p. 18.

Rulemaking,[2] but concluded that the purported adverse effects stemmed from an unreasonable interpretation of the Purpose Limitation:

> The Acting Register agrees with opponents that the [Purpose] Limitation is not properly read to prohibit teaching, academic dialogue, or scholarship involving information derived from good-faith security research. In the 2015 Recommendation, the Register expressly found that the exemption was "likely to increase the use of works in educational settings" and that "teaching and scholarship would be enhanced" by it. She also noted that "[t]he desired research activities may result in criticism or comment about [a] work and the devices in which it is incorporated, including potential flaws and vulnerabilities." As those findings recognize, the focus of the [Purpose] Limitation is 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 [Purpose] 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. The Acting Register accordingly concludes that this requirement is unlikely to have an adverse effect on good-faith research, and therefore she does not recommend its removal.[3]

Because the adverse effects cited by Petitioners in support of removing the Purpose Limitation rely on a misreading of the Purpose Limitation, the Register should once again decline to recommend its removal from the existing security research exemption.

2. Security Limitation

The Security Limitation requires beneficiaries of the exemption to ensure that "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 operates, or those who use such devices or machines, and is not used or maintained in a manner that facilities copyright infringement." Petitioners characterize the Security Limitation as ambiguous because "a narrow reading might interpret 'primarily' to mean 'only'" and suggest that it will have an adverse effect on the ability of beneficiaries to "[engage] in scholarship which does not directly improve the security of devices, but rather contributes to scientific discussion."[4] Petitioners relied on similar reasoning to support removal of the Security Limitation during the 2018 rulemaking cycle. However, the Acting Register of Copyrights concluded that such a reading of the Security Limitation was unreasonable:

> The Acting Register finds no realistic likelihood of adverse effects based on proponents' first two arguments. First, it is not plausible to conclude that the term "primarily" could be interpreted to

[2] During the 2018 Rulemaking cycle, the Acting Register of Copyrights referred to the Purpose Limitation as the "Access Limitation." *See* 2018 Recommendation at pg. 286 ("They object to the two references to "solely"—the requirement that circumvention be "solely" for the purpose of good-faith security research, and the definition of such research as accessing a program "solely" for purposes of good-faith testing, investigation, and/or correction (the 'Access Limitation')."").

[3] 2018 Recommendation at pg. 305.

[4] Halderman, CDT, ACM Petition at p. 21.

> mean "only." Those two terms clearly are not synonymous, and nothing in the record suggests that any copyright holder has advanced such a reading. Likewise, proponents' concern that the exemption might not extend to situations in which a researcher advises against the use of a device seems farfetched. It would be absurd to construe the exemption to mean that research is protected only if it results in users being able to use the class of devices whose security or safety is being examined.[5]

Consistent with the reasoning from 2018, we urge the Register not to recommend removal of the Security Limitation.

3. Lawfully Acquired Limitation

The Lawfully Acquired Limitation provides that circumvention can be undertaken only on a "lawfully acquired device or machine." Petitioners assert that the Lawfully Acquired Limitation chills good-faith security research of devices acquired on the secondary market because "security researchers cannot know for sure whether the seller had placed such a resale constraint on the original buyer."[6] They argue, for instance, that disputes over the "lawfully acquired" requirement could arise if a researcher obtains a device on the secondary market from a seller who is violating the terms of a license with the original vendor. Here, too, Petitioners rely on an interpretation of the 2018 Exemption that the Acting Register of Copyrights deemed unreasonable:

> The Acting Register is not convinced that this provision risks chilling good-faith research. There is no indication in the record that any disputes of the type described by proponents have arisen, and speculation alone is insufficient to demonstrate a likely adverse effect. Furthermore, the Acting Register does not believe the language to be ambiguous: it 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. In any event, to avoid uncertainty, the Acting Register now makes clear her understanding that the phrase "lawfully acquired" requires only that the acquisition not be in violation of law. The Acting Register thus agrees with CCIPS that eligibility for the exemption "should not turn on restrictive contractual terms purporting to limit use of the hardware on which the copyrighted software is running." The Acting Register believes this guidance obviates any need for amending the regulatory text.[7]

Because Petitioners' argument relies on an unreasonable interpretation of the Lawfully Acquired Limitation, the Register should again decline to endorse its removal.

4. Other Laws Limitation

The Other Laws Limitation provides that circumvention must "not violate any applicable law, including without limitation the Computer Fraud and Abuse Act." Petitioners' core argument is that the Other Laws Limitation imports ambiguity into the exemption that chills good-faith security research because beneficiaries must solicit counsel to determine whether their project may implicate a wide variety of "legal regimes including—but not limited to—the DMCA, the CFAA, the Wiretap Act, various federal and state level privacy laws, and

[5] 2018 Recommendation at pg. 309.
[6] Halderman, CDT, ACM Petition at p. 24.
[7] 2018 Recommendation at pg. 303.

every state's contract law."[8] In considering a similar argument during the 2018 Rulemaking, the Acting Register of Copyrights concluded that Petitioners had failed to demonstrate a causal connection between the purported adverse effect and the Other Laws Limitation:

> Taking all of these considerations into account, the Acting Register concludes that proponents have failed to establish an adverse effect resulting from this provision. As the Office recently noted in the context of section 1201(j), "it [is] not clear . . . that the requirement to comply with other laws impedes legitimate security research; other laws still apply even if the activity is permitted under section 1201. Nor did proponents offer a persuasive response to opponents' contention that section 1201 is not the cause of any adverse effect when circumvention is prohibited by other laws.[9]

Petitioners also contend that inclusion of the Other Laws Limitation exceeds the Copyright Office's rulemaking authority because the "[importation of] extraneous legal regimes into the analysis for an exemption to 1201 positions the Office to effectively rule on the contours of non-copyright laws that lay entirely outside the ambit of the Office's limited delegated authority."[10] However, in conditioning eligibility for the security exemption on the Other Laws Limitation, the Copyright Office is relying on the very statute that is the basis of its rulemaking authority. As the Acting Register of Copyrights observed during the 2018 Rulemaking, the Other Laws Limitation was incorporated into the security research exemption in an effort to ensure that it would be faithful to Congressional intent:

> In addition, the Acting Register finds it significant that Congress included an obligation to comply with other laws in the statutory provision speaking most directly to the activity at issue here. While the proposed exemption does differ from the statute in various respects, the Acting Register believes it appropriate to track the statutory language to the extent possible, "in the interest of adhering to Congress's basic purpose in section 1201(j).[11]

Furthermore, the statutory remit of Section 1201 expressly invites the Librarian of Congress and Copyright Office to consider non-copyright interests that are relevant to proposed exemptions. In addition to copyright-related considerations, Section 1201 grants the Librarian of Congress the authority to consider "other factors" that may be relevant to the consideration of a proposed exemption.[12] The Copyright Office has rightly concluded that "the open-ended nature of this statutory factor permits broad consideration of a wide variety of factors," and indeed "non-copyright concerns have been consistently relevant to proposed exemptions in past rulemakings, such as competition and telecommunications policies supporting past cellphone unlocking exemptions."[13] Accordingly, we urge the Copyright Office to again recommend retention of the Other Laws Limitation.

---

[8] Halderman, CDT, ACM Petition at p. 25.
[9] 2018 Recommendation at pg. 311.
[10] Halderman, CDT, ACM Petition at p. 26.
[11] 2018 Recommendation at pg. 311
[12] Section 1201(a)(1)(C)(5)
[13] See U.S. COPYRIGHT OFFICE, SECTION 1201 OF TITLE 17 at pg. (2017) a, https://www.copyright.gov/policy/1201/section-1201-full-report.pdf

5. Good-Faith Privacy Research

The Software Freedom Conservancy urges the Copyright Office to recommend an expansion of the definition of "good-faith security research" so that the exemption extends to circumvention undertaken for "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." While "security research" and "privacy research" may bear some similarities in certain circumstances, their petition acknowledges that the activity for which it is seeking an exemption is fundamentally different in kind than the activity currently covered by 37 C.F.R. § 201.40(b)(11).[14] Unlike the security research exemption, the Software Freedom Conservancy seeks an exemption to "permit consumers to 'remove software or disable functionality that may expose personal information'"[15] regardless of whether the exposure relates to any unintended security flaw or vulnerability. Moreover, whereas 37 C.F.R. § 201.40(b)(11) is intended to address ambiguities in Section 1201(j), the Software Freedom Conservancy acknowledges that it is seeking is an exemption to address ambiguities arising under Section 1201(i).[16]

Given the different intended scopes of these provisions, we have concerns with the Software Freedom Conservancy's proposal. The security research exemption reflected in 37 C.F.R. § 201.40(b)(11) incorporates a number of considerations and safeguards that reflect an effort to address the needs of the security research community while remaining faithful to the congressional intent reflected § 1201(j).[17] Thus, while we are not opposed in

[14] *See* Software Freedom Conservancy Petition at pg. 7 ("While privacy research and security research often overlap, valuable privacy research may not always meet the criteria for the exemption at 37 C.F.R. § 201.40(b)(11), because investigating how a product or service collects and disseminates consumer information may not relate to any 'security flaw or vulnerability.' Rather, privacy researchers often aim to investigate and raise awareness about the intended (although obscured or undocumented) functioning of a particular product or service.").

[15] Software Freedom Conservancy Petition at pg. 2.

[16] Id. ("As to Conservancy's request for an expansion of the good-faith security research exemption to permit consumers to "remove software or disable functionality that may expose personal information," we recognize that 17 USC § 1201(i) addresses such end-user mitigations and is the more appropriate focus of any proposed expansion to those protections. Conservancy discusses the limitations of § 1201(i) below and suggests that the Office recommend legislation to expand § 1201(i) to address these concerns rather than expanding the good-faith security research exemption to do so.").

[17] See, e.g., 2018 Recommendation at pg. 304 ("[T]he Acting Register believes that any exemption authorizing this activity should require such authorization. Such a requirement is consistent with congressional intent as reflected in the permanent exemption for security testing under section 1201(j), which is conditioned upon the user obtaining "the authorization of the owner or operator of [the] computer, computer system, or computer network" that will be accessed); 2018 Recommendation at pg. 309 ("The Acting Register nevertheless does not believe removal of this provision to be advisable. In 2015 the Register recommended adoption of this language—which tracks the statutory factors governing eligibility for the security testing exemption under section 1201(j)1877—because she determined that it reflected congressional intent regarding appropriate disclosure requirements in this context.1878 The Acting Register adheres to that view."); 2018 Recommendation at pg. 311 ("In addition, the Acting Register finds it significant that Congress included an obligation to comply with other laws in the statutory provision speaking most directly to the activity at issue here.1891 While the proposed exemption does differ from the statute in various respects, the Acting Register believes it appropriate to track the statutory language to the extent possible, "in the interest of adhering to Congress's basic purpose in section 1201(j).").

principle to a separate exemption to enable good-faith privacy research, the Copyright Office should decline to expand the 2018 Exemption for the purposes of addressing concerns that are orthogonal to the security concerns on which this proceeding is focused.

DOCUMENTARY EVIDENCE

Commenters are encouraged to submit documentary evidence to support their arguments or illustrate pertinent points concerning the proposed exemption. Any such documentary evidence should be attached to this form and uploaded as one document through regulations.gov.