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

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

ITEM A. COMMENTER INFORMATION

The petitioner is Software Freedom Conservancy (Conservancy), a not-for-profit organization that helps to promote, improve, develop, and defend Free and Open Source Software (FOSS)—software developed by volunteer communities and licensed for the benefit of everyone. Conservancy is the nonprofit home for dozens of FOSS projects representing well over a thousand volunteer contributors. Our communities maintain some of the most fundamental utilities in computing today, and introduce innovations that will shape how software will be created in the future.

Conservancy fights for software freedom, which gives people control over the functionality of the software they use, including the freedom to add or remove features. One of the most important aspects of this control is allowing individuals to determine when and how private information is sent to other people or companies. Because of this, Conservancy naturally cares deeply about privacy for all software users. While our ultimate organizational goal is to preserve all software freedom for everyone, the ability to protect one's own privacy is one of the most essential rights in the entire group of rights that software freedom activists seek. Conservancy is at the forefront of non-profit organizations in making practical progress toward a future where people can correct and improve the software in devices they own, in large part to improve their privacy while using these devices.

Conservancy may be contacted as follows:

Karen Sandler, Executive Director
Software Freedom Conservancy, Inc.
137 Montague St., Ste.
380 Brooklyn, NY 11201-3548
dmca-exemption@sfconservancy.org
+1-212-461-3245

ITEM B. PROPOSED CLASS ADDRESSED

Proposed Class 13: Computer Programs—Security Research

ITEM C. OVERVIEW

Conservancy initially proposed an expansion of the "good-faith security research" exemption, 37 C.F.R. § 201.40(b)(11), to encompass circumvention of technological protection measures (TPMs) protecting computer programs for the purpose of "good-faith testing, investigation, and/or correction of privacy issues (including flaws or functionality that may expose personal information)."[1]

While no respondents wholly opposed Conservancy's proposal of privacy-research exemption, their comments raised thoughtful concerns about addressing privacy and security research in a single exemption.[2] Conservancy therefore agrees with respondent BSA | The Software Alliance ("BSA") that a better approach would be to establish a new, separate exemption for privacy research, modeled on the security research exemption and incorporating similar limitations. As the BSA observes, this approach would create the same symmetry between the new privacy research exemption and the statutory exemption at Section 1201(i) as already exists between the security research exemption and Section 1201(j).

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

As detailed in our initial comment, the technological protection measures ("TPMs") at issue include encryption, code obfuscation, protected memory spaces, and disabled physical access ports.[3] Circumvention techniques include decompilation and de-obfuscation of software applications, decryption of firmware and datastreams, and accessing disabled ports on device circuit boards.[4]

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

The BSA, while "not opposed in principle to a separate exemption to enable good-faith privacy research," objects to incorporating this exemption into the existing security research exemption.[5] Its reasons are sound: that exemption was crafted to include limitations specific to security research, and to work in tandem with Section 1201(j), which exempts authorized security testing.[6] Rather than upset this balance, Conservancy agrees with BSA that a separate exemption should be established for privacy research.

A separate exemption will enable the Register to balance the exemption for privacy research against the related statutory exemption in Section 1201(i), as it has done with the security research exemption and Section 1201(j). It will also ensure that the consideration of proposals affecting one exemption—such as the pending petition by Prof. Halderman et al. to expand the security research exemption—are not unnecessarily complicated by its combination with the other.

[1] *See* Conservancy, Class 13 Comment at 2.
[2] *See* BSA, Class 13 Opposition at 7; Joint Creators, Class 13 Opposition at 7.
[3] *See* Conservancy, Class 13 Comment at 3-4.
[4] *Id*.
[5] *See* BSA, Class 13 Opposition at 7-8.
[6] *Id*.

Nonetheless, the exemption could be closely modeled on the current language of the security research exemption. We propose an exemption permitting circumvention of TPMs controlling access to:[7]

> (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 privacy 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, "good-faith privacy research" means accessing a computer program solely for purposes of good-faith testing, investigation, and/or mitigation of functionality capable of collecting or disseminating personally identifying information reflecting the activities of a natural person, 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 privacy of the general public, or users of the class of devices or machines on which the computer program operates, and is not used or maintained in a manner that facilitates copyright infringement.

This suggested language incorporates the same safeguards as the security research exemption, precluding unlawful, harmful, and infringing applications. It also adopts some of the terminology of the 1201(i) statutory exemption, reflecting the interdependence of the two exemptions.

The proposed exemption could not, however, incorporate all of Section 1201(i)'s limitations while still serving its purpose. For example, Section 1201(i) permits circumvention only where "the technological measure, or the work it protects, collects or disseminates personally identifying information about the person who seeks to gain access to the work protected."[8] As we noted in our initial comment, applying this limitation to privacy researchers would impede publicly minded research.[9]

Likewise, Section 1201(i) does not permit circumvention for the purpose of accessing a work "that does not collect or disseminate personally identifying information and that is disclosed to a user as not having or using such capability."[10] But as our petition demonstrates, much privacy research work is aimed at confirming or falsifying such claims.[11] If the legality of

[7] In answer to the Joint Creators and Copyright Owners' question, the scope of "computer programs" would not be limited to embedded device firmware, though our initial comments may have focused there. Joint Creators and Copyright Owners, Class 13 Comment at 7.
[8] 17 U.S.C. § 1201(i)(1)(B).
[9] Conservancy, Class 13 Comment at 7-8.
[10] 17 U.S.C. § 1201(i)(2).
[11] Conservancy, Class 13 Comment at 3.

such research depended on whether the claims turned out to be true, researchers performing socially valuable work would be compelled to give up their work or risk their liberty.

The other comments responding to Conservancy's petition are concerned with our suggestion that Section 1201(i) be expanded to give consumers more latitude to fix privacy issues in products they own.[12] Because statutory exemptions are not subject to amendment via this rulemaking process and our proposal for a privacy research exemption does not depend upon changes to Section 1201(i), we do not address those comments here.

DOCUMENTARY EVIDENCE

N/A

[12] *See* Conservancy, Class 13 Comment at 9-10; Joint Creators, Opposition at 7; Motor & Equipment Manufacturers Association, Opposition at 1.