UNITED STATES COPYRIGHT OFFICE

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

Reply Comment of Matthew Green Regarding Proposed Class 10

ITEM A. COMMENTER INFORMATION

Commenter:

Matthew Green

Representative:

Electronic Frontier Foundation
Kit Walsh, Senior Staff Attorney
Counsel to Professor Green
815 Eddy Street
San Francisco, CA 94109
415 436 9333
kit@eff.org

ITEM B. PROPOSED CLASS ADDRESSED

Proposed Class 10: Computer Programs—Security research

ITEM C. OVERVIEW

Security research is essential to the well-being of those who are subject to digital technology. The existing permanent and temporary exemptions for security research are unnecessarily limited and harm the public by inhibiting important, noninfringing security research. In particular, the limitation of the temporary exemption to "a device or machine that is primarily designed for use by individual consumers" fails to alleviate the adverse impact of the ban on circumvention on research into a variety of devices on Green's research agenda.

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

See initial filing.

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

I. Ownership of a Copy of Software is Not Required to Make Noninfringing Uses

Fair use does not require a user to own or license a copy of a work; to the contrary, the fair use doctrine specifically ensures that the public may use the work in many ways without permission from the copyright holder. Nor, under prevailing law, may a contractual agreement such as an end-user license agreement impose liability under *copyright* law for conduct that is

noninfringing, such as fair use.[1] The Register has acknowledged that "[a]llowing form agreements that are not subject to individual negotiation to extend copyright liability to activities that would otherwise be noninfringing could disrupt carefully balanced legislative policy choices, including about what kinds of activities should trigger potentially large statutory damages or attorney's fee awards." Software Enabled Consumer Products Report, at 67.

The Register, therefore, need not determine who 'owns' copies of the software on those devices. The fair use status of research testing those copies does not depend on whether the researchers are also owners.

However, in addition to fair use, owners of copies of software benefit from the overlapping legal protection of Section 117. Should the Register find it necessary to decide the issue, it should recognize that the owner of a physical device is typically also the owner of the copy of the software needed to operate that device and make it useful.

Under *Krause v. Titleserv*,[2] the relevant question is whether a party "exercises sufficient incidents of ownership over a copy of that program to be considered the owner[.]"[3] *Vernor* alternatively provides that "a software user is a licensee rather than an owner of a copy here the copyright owner (1) specifies that the user is granted a license; (2) significantly restricts the user's ability to transfer the software; and (3) imposes notable use restrictions upon the user."[4]

A researcher who lawfully acquires a device typically pays substantial consideration and gains possession of the device. The copies of software that operate the device operate for the benefit of purchaser or at their direction, not the original rights-holder. The purchaser may typically dispose of the device whenever they wish. Manufacturers generally do not retain the right to repossess software copies from their purchasers. Opponents have not argued to the contrary for the use cases Green has identified.

If narrow categories of devices do exist where these ownership-limiting properties are present, that does not defeat the general conclusion that the software on devices investigated by security researchers is likely to be 'owned' by the owner of the device.

II. Scope of Devices

Opponents propose a distinction between consumer devices and "critical infrastructure". There are two main problems with this approach.

First, as a taxonomy it is incomplete. Many devices do not clearly fall into either of those categories. Attempting to apply that binary classification to the uses Green proposes does not yield clear results. For instance, are hardware encryption modules "critical infrastructure"? Toll

---

[1] *Blizzard v. MDY Indus., LLC*, 629 F.3d at 941 (enabling a rightsholder to "designate any disfavored conduct during software use as copyright infringement . . . would allow software copyright owners far greater rights than Congress has generally conferred on copyright owners").
[2] 402 F.3d 119 (2d. Cir. 2005).
[3] *Krause*, 402 F.3d at 124.
[4] *Vernor v. Autodesk, Inc.,* 621 F.3d 1102, 1111 (9th Cir. 2010).

collection systems? The Register should not adopt limitations that make it difficult for the public to understand what is permitted and what is not.

Second, opponents do not explain why the owners of "critical infrastructure" should be barred from identifying and fixing security vulnerabilities. As has been extensively discussed in this rulemaking, independent analysis promotes security by bringing more expertise to bear, by holding manufacturers accountable, and removing barriers to swift correction of security vulnerabilities.

III. Limitations Not Rooted in Copyright Concerns

The Office has recognized that the non-copyright-related "health, safety, and environmental concerns" should be addressed as needed by regulations outside of Title 17.[5] The security research exemption issued in 2015 was improperly limited by such considerations, and those limitations should be removed.

For instance, it is illogical for Section 1201 liability to hinge on whether research presents a risk of torts for which there is already an adequate legal remedy outside of Title 17. A rightsholder is not harmed in such a scenario; a separate cause of action for them under Section 1201 is an unjustified windfall, an over-deterrent, and an impediment to settlement among the parties truly involved in the event a researcher causes injury to a third party.

The rulemaking concerns liability under a particular provision of the DMCA; it is not and should not be an open-ended forum for generally governing the conduct of technology users. If the Office is concerned that the public will view it as such, it can reiterate that the exemptions do not excuse anyone from complying with other provisions of law.

IV. "Sole Purpose" Language in Exemptions Endangers Legitimate Research

The 2015 rulemaking exemption suffered from strict technical requirements combined with vague restrictions. Research must be conducted "solely" for the listed purposes, and the acts of third parties outside of a researcher's control may arguably disqualify the researcher from the exemption's protection. "Sole purpose" language threatens to disqualify researchers who have other valid purposes, while liability for acts of third parties should be handled under doctrines of secondary liability, not as redundant and vague restrictions on exemptions to Section 1201.

[5] Copyright Office, "Section 1201 of Title 17," June 2017, at 126.