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 over 5,000 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.

Among the projects for which Conservancy provides logistical, administrative, and legal support are OpenWrt and BusyBox. OpenWrt produces an embedded operating system for routers that can be installed in place of the stock firmware on commercially available routers. BusyBox provides a number of key system utilities that enable such devices to run applications, interact with files, access network services, and more. Conservancy also represents the interests of a coalition of contributors to the Linux kernel. Both BusyBox and Linux are core components of the operating system of OpenWrt and most consumer routers.

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 11: Computer Programs—Jailbreaking

To enable the installation of alternative firmware in routers and other networking devices.

ITEM C. OVERVIEW

Conservancy proposed an exemption permitting jailbreaking of wireless routers and other networking devices for the purpose of installing alternative operating system software. As we detailed in our initial comment, the proposed exemption would enable the owner of a router to "improve the router's performance, reliability, and security, expand its capabilities, and extend its useful life."[1]

Two commenters oppose the proposed exemption: ACT | The App Association ("ACT") and the "Joint Creators and Copyright Owners," comprising the Motion Picture Association, Inc. ("MPA"), the Alliance for Recorded Music ("ARM"), and the Entertainment Software Association ("ESA"). Both submissions focus primarily on an unrelated petition proposed by the Electronic Frontier Foundation's ("EFF") to permit jailbreaking of streaming devices. The comments address Conservancy's proposal only as an afterthought, citing no law or evidence specific to Conservancy's arguments.

As an initial matter, it is unclear what stake either group has in the proposed exemption. According to its website, ACT "represents more than 5,000 app makers and connected device companies in the mobile economy."[2] As its comments make clear, its members develop applications that are delivered via "curated platforms (e.g., Apple's App Store, Google Play for mobile, Steam for games)" on mobile devices and home entertainment systems.[3] ACT claims that "App Association members compete in the firmware marketplace" but presents no evidence that its members develop applications for routers and networking devices, which do not use app stores or similar "curated platforms" for content delivery.[4]

Likewise, the Joint Creators and Copyright Owners represent producers of content—motion pictures, music, and video games—that is not played on routers. They cite no evidence that jailbreaking a router facilitates infringement of their members' content, or that they represent the interests of any producer of routers or router firmware. Instead, their brief treatment of Conservancy's proposal repeatedly cites their discussion of EFF's proposed exemption, and leaves the connection between them as an exercise for the reader.

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

As discussed more fully in Conservancy's initial comment, the technological protection measures at issue include firmware encryption and administrative controls. Depending on the device, circumvention may require exploiting software security vulnerabilities, reverse-engineering manufacturers' encryption schemes and using them to encrypt user-supplied firmware files, or accessing physical interfaces on the device's circuit board.[5]

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

A. The proposed exemption would not facilitate infringement

[1] Conservancy, Class 11 Long Comment at 2-3.
[2] ACT | The App Association, About, https://actonline.org/about-3/.
[3] *See* ACT, Class 11 Opposition at 4-5.
[4] *Id* at 5.
[5] *See* Conservancy, Class 11 Comment at 3-4.

The Joint Creators first argue that Conservancy's proposal raises "the same concerns expressed above regarding the facilitation of infringement," referring indistinctly to its arguments against EFF's proposed jailbreaking exemption for video-streaming devices.[6] But those concerns were peculiar "devices that transmit content to televisions"[7] and are designed to play the content produced by their members. Routers and other networking devices possess neither the video outputs required to "transmit content to televisions," nor the processing power to run video-streaming applications.[8] Neither opponent presents any examples of routers being modified to facilitate infringement, nor is Conservancy aware of any.

B. Market alternatives are not a substitute for the proposed exemption

Both ACT and the Joint Creators argue that the marketplace provides adequate alternatives for consumers who wish to run FOSS operating systems on their routers. ACT claims that "[w]hile proprietary firmware and computer programs are used by some manufacturers, there are extensive open-source options available," though does not cite a single example.[9] The Joint Creators liken the proposed exemption to one opposed by the Register's 2010 recommendation, which would have permitted users of Linux PCs to circumvent DVD copy protection for the purpose of watching DVDs on their operating system of choice.[10]

These arguments overlook key points raised in Conservancy's initial comment. First, even "proprietary" router firmwares are built from FOSS components like the Linux kernel and BusyBox.[11] Unlike the producers of a typical DVD, the authors of these components encourage modification and reuse via FOSS licenses. Given the express authorization of these authors and the lack of any opposition by router manufacturers, the opposition of the Motion Picture Association should be of little consequence—particularly when respondents have cited no evidence that the exemption would encourage infringement of their members' works.

Second, the availability of FOSS-friendly routers on the market is irrelevant to many of the non-infringing uses cited in our initial comment. The owner of a router should be permitted to extend that device's functionality or improve its security by installing a new operating system regardless of whether buying a new router would achieve the same end. Prohibiting these

---

[6] *See* Joint Creators, Class 11 Opposition at 7.
[7] *Id*.
[8] *See* Lewin Day, *Up Your Home Network Performance – Build Your Own Router!*, Hackaday, June 19, 2020, https://hackaday.com/2020/06/19/up-your-home-network-performance-build-your-own-router/ ("The main problem with commodity routers is a lack of processing power.").
[9] *See* ACT, Class 11 Opposition at 3.
[10] *See* Joint Creators, Class 11 Opposition at 7 & note 29 (citing RECOMMENDATION OF THE REGISTER OF COPYRIGHTS IN RM 2008-8; RULEMAKING ON EXEMPTIONS FROM PROHIBITION ON CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS FOR ACCESS CONTROL TECHNOLOGIES at 220 (2008)).
[11] *See* Conservancy, Class 11 Comment at 2 & note 1 (listing FOSS source code download links for several major router manufacturers). *See, e.g.*, Cisco, Open Source Used in Cisco CVR100W 1.0.1.22 at 2-3, https://www.cisco.com/c/dam/en_us/about/doing_business/open_source/docs/Cisco_CVR100W_1_0_1_22.pdf (listing 40 FOSS components used in a Cisco router).

commonsense modifications will only encourage consumers to keep their insecure and obsolete devices longer, or consign them to a landfill sooner.[12]

C. Existing exemptions are inadequate

The Joint Creators contend that "to the extent security or privacy concerns are at issue, the statutory exceptions in Sections 1201(g), 1201(i) and 1201(j), alongside the existing security research exemption, should provide sufficient cover to inspect/alter routers."[13] Conservancy identified several noninfringing uses unrelated to privacy and security concerns, including research to advance networking technology, improvements to network performance, implementation of parental controls, and upgrades to new network protocols, none of which would be covered by these exemptions.[14] But even the proposed privacy- and security-related uses are not adequately addressed by existing exemptions.

Section 1201(g) exempts "encryption research," defined as "activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products."[15] This exemption does not relate to any of the noninfringing uses for which Conservancy seeks an exemption.

Section 1201(j) exempts "security testing," so long as it's "solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability."[16] The security research exemption currently codified at 37 CFR § 201.40 expands upon the protections of Section 1201(j), permitting researchers to probe the security of computer programs for the benefit of the public, and not only their own systems.[17]

While many of the noninfringing uses enabled by the proposed exemption would promote the security of network devices, consumers cannot rely upon these limited exemptions even for those purposes. As our comment demonstrates, consumer routers receive firmware updates infrequently, and all of them are subject to multiple critical security vulnerabilities.[18] But it's effectively impossible to upgrade only the vulnerable components, because upgrading one component typically requires upgrading related components,[19] and most routers require updating the entire firmware as a package.[20] For this reason, a user concerned with the security of their networking device can rarely "solely" correct its security flaws, and is often left with no other

[12] *See* Alana Semuels, *The World Has an E-Waste Problem*, Time.com, May 23, 2019, https://time.com/5594380/world-electronic-waste-problem/ (reporting that "50 million tons of e-waste [were] generated globally" in 2018).
[13] Joint Creators, Class 11 Opposition at 7.
[14] Conservancy, Class 11 Comment at 5-7.
[15] 17 U.S.C. § 1201(g).
[16] 17 U.S.C. § 1201(j).
[17] 37 CFR § 201.40.
[18] *Id* at 7.
[19] *See* Dependency hell, Wikipedia, https://en.wikipedia.org/wiki/Dependency_hell.
[20] *See* Firmware – Flashing, Wikipedia, https://en.wikipedia.org/wiki/Firmware#Flashing.

option than to install a frequently updated FOSS operating system firmware like the Linux- and BusyBox-based OpenWrt.

Finally, Section 1201(i) permits circumvention for the purpose of preventing a work from collecting or disseminating personally identifying information about the person doing the circumventing.[21] While certain of the noninfringing uses we cite relate to protection of privacy, they do not fit within this exemption's narrow limits. Enabling a virtual private network or enabling DNS encryption on a router, for example, would protect the privacy of everyone on the network, not only of "the person who seeks to gain access to the work protected."[22]

D. Conclusion

Both ACT and the Joint Creators attack Conservancy's proposal by cut-and-paste, merely repeating their criticisms of EFF's proposed exemption for streaming devices without citing evidence applicable to routers. While ACT "encourages the Copyright Office to learn more about the firmware marketplace before assuming that adopting the proposed new exemption for routers and non-integrated streaming devices would not have a negative impact," it does not offer any such education in its comments.[23] Since neither opponent cites any evidence that the proposed exemption would enable infringement, the exemption should be granted.

DOCUMENTARY EVIDENCE

N/A

[21] 17 U.S.C. § 1201(i).
[22] *See* Conservancy, Class 11 Comment at 5; 17 U.S.C. § 1201(i)(1)(B).
[23] *See* ACT, Class 11 Opposition, at 5.