U.S. Department of Justice

Criminal Division

Computer Crime and Intellectual Property Section *Washington, D.C. 20530*

February 9, 2021

Regan Smith
General Counsel and Associate Register of Copyrights
Library of Congress
Copyright Office
101 Independence Avenue, SE
Washington, DC 20559-6000

Dear Ms. Smith:

The Computer Crime and Intellectual Property Section (CCIPS) of the United States Department of Justice submits these comments in response to the Copyright Office's Notice of Proposed Rulemaking (NPRM), its Eighth Triennial rulemaking proceeding under the Digital Millennium Copyright Act (DMCA).[1] Specifically, CCIPS offers these comments with regard to the existing DMCA exemption permitting circumvention for purposes of good-faith security research (codified at 37 CFR 201.40(b)(11)) and two petitions for Proposed Class 13, Computer Programs—Security Research, seeking to expand the existing exemption: (1) the petition from Professor J. Alex Halderman, the Center for Democracy and Technology, and the Association of Computing Machinery ("Halderman petition")[2]; and (2) the petition from the Software Freedom Conservancy ("SFC petition").[3] For the reasons set forth below, CCIPS supports renewal of the existing exemption for good-faith security research, as well as some further expansion and clarification of that exemption, but does not support either of the proposals in its entirety.

The U.S. Department of Justice and the DMCA

As outlined in CCIPS's letter of June 28, 2018 as part of the Copyright Office's Seventh Triennial rulemaking proceeding on the DMCA, the U.S. Department of Justice, and CCIPS in particular, occupies a unique position with respect to the DMCA's anti-circumvention provisions

[1] Library of Congress, Copyright Office, Notice of Proposed Rulemaking, Exemptions to Permit Circumventions of Access Controls on Copyrighted Works, 85 Fed. Reg. 65,293, 65,310 (Oct. 15, 2020) ("NPRM").
[2] Prof. J. Alex Halderman, Center for Democracy & Technology, and Association of Computing Machinery, Petition for New Exemption Under 17 USC § 1201, https://www.copyright.gov/1201/2021/petitions/proposed/New%20Pet.%20-%20J.%20Alex%20Halderman%20et%20al.pdf
[3] Software Freedom Conservancy, Inc., Petition for New Exemption Under 17 USC § 1201, https://www.copyright.gov/1201/2021/petitions/proposed/New%20Pet.%20-%20Software%20Freedom%20Conservancy%20-%202.pdf

and computer security. The Department is responsible for criminal enforcement of a range of statutes protecting intellectual property, including enforcement of the DMCA's criminal provision (17 U.S.C. § 1204), which apply to willful violations of the anti-circumvention provisions in Section 1201 committed for purposes of commercial advantage or private financial gain. As part of the Department's Criminal Division, CCIPS advises other federal prosecutors on the application of the DMCA, and has brought criminal DMCA charges in a variety of cases involving circumvention of technological protection measures and trafficking in devices designed or marketed for use in circumvention.

In addition to its role in criminal enforcement of the DMCA and other intellectual property laws, the Department is responsible for prosecuting federal crimes involving unauthorized access to computers, damage to information systems, and other offenses under the Computer Fraud and Abuse Act (CFAA), among other statutes. CCIPS advises other federal prosecutors on the application of the CFAA, and is involved, along with other Department of Justice components, in litigation concerning the interpretation of the CFAA, including *Van Buren v. United States*,[4] currently before the Supreme Court. In support of that work, CCIPS maintains a Cybersecurity Unit focused specifically on cybersecurity issues, including improving computer security practices, awareness of and defense against security vulnerabilities, and data breach response. As a result, the Department is keenly aware of the harms that can result from exploitation of technological vulnerabilities in software, as well as the benefits that legitimate security research provides to the government and the public by identifying vulnerabilities in software, devices, and networks and defending such systems from criminal exploitation.

CCIPS recognizes the important role the DMCA plays as a legal reinforcement of technological measures that protect copyrighted works, but we also recognize that the statutory prohibitions set forth in 17 U.S.C. § 1201 are broad. Because some circumventions of technological protection measures can provide enormous public benefit with little or no impact on copyright protection, the exceptions set forth in the statute itself, as well as those developed through the Copyright Office's triennial rulemaking process, are essential. These exceptions ensure that the DMCA does not penalize or discourage legitimate activity that serves the public interest, particularly where that activity does not involve or facilitate the infringement of copyright.

In the previous triennial rulemaking process in 2018, CCIPS submitted comments that, among other things, expressed support for a limited expansion of the exemption for computer security research effective at the time, which the Copyright Office had first adopted in 2015.[5] The Copyright Office adopted an expanded version of the research exemption in 2018, codified in 37 C.F.R. § 201.40(b)(11). CCIPS supports the renewal of that exemption.

---

[4] *Van Buren v. United States*, No. 19-783 (filed December 18, 2019)

[5] Codified at the time at 37 CFR 201.40(b)(7) (2015)

The Halderman Petition

In the current rulemaking process, the Halderman and SFC petitions each propose to expand further the existing exemption for computer security research. The Halderman petition proposes to remove several limitations in the current exemption. First, it proposes to remove the requirements that a circumvention must be carried out on a "lawfully acquired device or machine on which the computer program operates" and "not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986, as amended and codified in title 18, United States Code." The Halderman petition further proposes to remove the condition that to be exempted, a circumvention must be conducted "solely" for the purpose of good-faith research, and that "the information derived from the activity is used primarily to promote the security or safety of [the class of devices or their users] and is not used or maintained in a manner that facilitates copyright infringement," in order to avoid what petitioners argue would be unconstitutional limits on post-circumvention speech.

In 2018, CCIPS commented on a similar proposal, also authored by Professor Halderman (with co-author Professor Ed Felten), to remove the "any applicable law" language from the security research exemption. We noted that, regardless of the scope of the DMCA or its exemptions, security researchers were already required to follow an array of laws and regulations that apply to their conduct, and quoted the Register's previous observation that the "other applicable laws" language should have little effect on the scope of permissible research because "other laws still apply even if the activity is permitted under section 1201."[6] We also explained that the DMCA, which prohibits circumvention of technological barriers to access copyrighted works, and the CFAA, which prohibits, among other things, circumvention of technological barriers to access computers and networks, potentially overlap in their application. In turn, we expressed our concern that the removal of the "other applicable laws" language, particularly its specific reference to the CFAA, might mislead researchers into believing that adherence to the conditions of the DMCA's research exemption would also serve to exempt those researchers from liability under the CFAA or other applicable laws. Although good faith computer security research should indeed comply with all applicable laws, we are now persuaded that replacing the existing requirement that research not violate "any applicable law" with alternative explanatory language would provide equally sufficient notice of the need to comply with applicable law. This change would also reduce the chance that potentially valuable research projects may be discouraged by fears that inadvertent or minor violations of an unrelated law could result in substantial liability under the DMCA.

To be clear, as part of the federal government's chief law enforcement body, we remain steadfast in our view that those who undertake computer security research in good faith can and should abide by all applicable federal, state, and local laws. These laws include not only copyright law, the DMCA, and CFAA, but also other laws unrelated to copyright or technology that nevertheless apply to security researchers, including employment and taxation laws. Researchers who violate the law intentionally should be held accountable for such violations, incurring whatever penalties the relevant jurisdiction has determined are appropriate for the

[6] CCIPS June 28, 2018 letter at 5, quoting the Copyright Office's 1201 Policy Study (June 2017) at 80.

violation in question.[7] Yet, as we noted in our 2018 comments, while the DMCA was enacted to serve the important goal of protecting technological measures and thereby bolstering protection for the exclusive rights granted by copyright, it was not designed to ensure compliance with other laws unrelated to copyright. It is neither the most efficient nor most appropriate tool for doing so. Unfortunately, conditioning the security research exemption on the requirement that the research "not violate any applicable law" effectively means that where a researcher has undertaken a project involving circumvention in good faith, after diligent efforts to ensure legal compliance, even a minor violation of applicable law could prevent the security research exemption from applying, and result in substantial liability under the DMCA. An increasing portion of contemporary computer security research involves collaboration among researchers across international borders. Accordingly, the "any applicable law" requirement means that a U.S. researcher's violation of foreign law could result in a loss of the exemption and attendant liability under the DMCA. This could be the consequence even where the foreign violation is an obscure or minor one, the foreign law in question is more onerous than or inconsistent with U.S. law, or the foreign law is administered or enforced in a manner inconsistent with U.S. standards. The existing language significantly increases the potential consequences to security researchers of even a minor violation of the law by exposing them to DMCA liability in addition to whatever penalty may apply directly to the violation. It thus may discourage valuable research projects that would otherwise be undertaken if researchers could be more certain the exemption would apply. Therefore, we would urge the Register to reassess the "any applicable law" language, and to consider replacing it with alternative text that would provide greater clarity and certainty to researchers hoping to operate under the exemption.[8]

In public comments on the Halderman petition,[9] the security firm Rapid7 proposes to strike the existing "any applicable law" language in 37 C.F.R. 201.40(b)(11)(i)[10] and replace it with alternative language in the definition of "good faith security research" in 201.40(b)(11)(ii) explaining that:

> Good faith security research that qualifies for the exemption under paragraph (a) may nevertheless incur liability under other applicable laws, including without limitation the Computer Fraud and Abuse Act of 1986, as amended and codified in title 18, United States Code.[11]

In our 2018 comments on the Felten/Halderman proposal striking the "any applicable law" language, we noted our concern that, in light of the frequent interplay between the DMCA and CFAA, striking the "any applicable law" language could be misunderstood to suggest that qualifying for the DMCA's research exemption would imply a similar exemption from the

---

[7] Failure to follow applicable laws, and especially flagrant disregard for applicable laws, may also suggest that research is not being carried out in good faith.

[8] We recognize that a similar requirement that good faith security *testing* not constitute "a violation of applicable law" is incorporated in the DMCA's statutory exception for security testing under § 1201(j)(2). One advantage of the Register's triennial review process, however, is that it permits the language of exemptions to adapt to evolving technologies, market conditions, and legal landscapes.

[9] Rapid7 comments - Eighth Triennial Proceeding, Class 13 (Dec. 14, 2020), p. 5.

[10] Striking the following from 37 CFR 201.40(b)(11)(i): "and does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986, as amended and codified in title 18, United States Code"

[11] Rapid7 comments at 5.

CFAA or other laws. However, Rapid7's proposed alternative language provides sufficiently clear notice to researchers that the CFAA and other laws continue to apply to research that qualifies for the DMCA exemption. We would recommend the Register consider appending further clarification that, "and qualification for the exemption under paragraph (a) is not a safe harbor or defense to liability under other applicable laws."

With regard to the Halderman petition's proposal to remove the "lawfully acquired" requirement from the security research exemption, we reiterate our 2018 comments regarding a similar proposal. The requirement that research be conducted on a device that is "lawfully acquired" serves the valid purpose of excluding research on devices obtained through theft or fraud, or conducted on other hardware or networks without permission of an owner or lawful operator. However, where good faith security research is not itself infringing, the question of whether such research is permissible under the DMCA should not turn on restrictive contractual terms purporting to restrict the use of the hardware on which the copyrighted software is running. We think the existing language, along with the Register's further clarification in 2018,[12] should be sufficiently broad to encompass research performed by a researcher who possesses a device legally, even pursuant to a license, and research performed on hardware owned by another party, if the researcher has the permission of the owner or another lawful possessor of the hardware, such as a lessee.

The Halderman petition further proposes to remove the term "solely" from 201.40(b)(11)(i) and (ii) and to remove from the definition of "good faith security" the requirement that "the information derived from the activity is used primarily to promote the security or safety of [the class of devices or their users] and is not used or maintained in a manner that facilitates copyright infringement." The petitioner argues such removal is necessary to avoid "unconstitutionally limiting post-circumvention First-Amendment-protected speech that includes information derived from good-faith security research." We are aware that the First Amendment implications of the research exemption were raised in *Green v. Department of Justice*, 392 F. Supp. 3d 68, 86 (D.D.C. 2019). We, however, do not agree that the DMCA or the existing language of the security research exemption violates the First Amendment. Accordingly, we do not believe that the either of these changes is necessary. To the extent that the existing language of 201.40(b)(11)(i) and (ii) could be construed to hold researchers responsible for copyright infringement committed by others, the Register's 2018 clarification—that "this language refers to the researcher's own use and maintenance of the information derived from the research," and that any facilitation should be assessed using established principles of third party liability for infringement—largely addressed this concern.[13]

The Software Freedom Conservancy Petition

The SFC petition proposes to expand the current exemption by clarifying that its definition of "good faith security research" includes "good-faith testing, investigation, and/or correction of privacy issues … and permits the owner of a device to remove software or disable functionality that may expose personal information." Although we recognize the importance of

[12] Recommendation of the Acting Register of Copyrights, Seventh Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Oct. 2018, p. 303.
[13] Recommendation of the Acting Register, at 309.

the type of testing and investigation concerning privacy issues, as Rapid7 noted in its comments on SFC's petition, these activities would seem to fall within the category of security testing already exempted by existing statutory and regulatory exemptions.[14] Therefore, we agree with Rapid7's recommendation that SFC's concerns could be more easily addressed through a clarifying statement and do not require changes to the wording of the security research exemption itself.

Conclusion

CCIPS appreciates the opportunity once again to contribute our views as part of the Copyright Office's triennial rulemaking proceeding under the DMCA. We appreciate the ongoing work of the Copyright Office to ensure the DMCA can continue providing effective legal protection for technologies to protect copyright works, while evolving to adapt to new technologies, uses, and users.

Sincerely,

John T. Lynch, Jr.

John T. Lynch. Jr.
Chief

[14] Rapid7 comments at 6.