UNITED STATES COPYRIGHT OFFICE

Petition for New Exemption Under 17 U.S.C. § 1201

8th Triennial Rulemaking

Please submit a separate petition for each proposed exemption.

NOTE: Use this form if you are seeking to engage in activities not currently permitted by an existing exemption. If you are seeking to engage in activities that are permitted by a current exemption, instead of submitting this form, you may submit a petition to renew that exemption using the form available at **https://www.copyright.gov/1201/2021/renewal-petition.pdf**.

If you are seeking to expand a current exemption, we recommend that you submit both a petition to renew the current exemption, and, separately, a petition for a new exemption using this form that identifies the current exemption, and addresses only those issues relevant to the proposed expansion of that exemption.

Item A. Petitioners and Contact Information

Please identify the petitioners and provide a means to contact the petitioners and/or their representatives, if any. The "petitioner" is the individual or entity proposing the exemption.

J. Alex Halderman
Professor of Computer Science & Engineering, University of Michigan
Director, University of Michigan Center for Computer Security and Society
Ann Arbor, MI
jhalderm@eecs.umich.edu

Represented by:
Samuelson-Glushko Technology Law & Policy Clinic at Colorado Law
Blake E. Reid, Director
Mikaela Colvin, Student Attorney
Boulder, CO
blake.reid@colorado.edu

Center for Democracy & Technology
Stan Adams, Open Internet Counsel and Deputy General Counsel
Washington, DC
sadams@cdt.org

U.S. Technology Policy Committee of the Association for Computing Machinery
James Hendler, Chair
Paul Hyland, Intellectual Property Subcommittee Chair
Washington, DC
acmpo@acm.org

Item B. Description of Proposed New Exemption

Provide a brief statement explaining the nature of the proposed new or expanded exemption. The information that would be most helpful to the Office includes the following, to the extent relevant: (1) the types of copyrighted works that need to be accessed; (2) the physical media or devices on which the works are stored or the services through which the works are accessed; (3) the purposes for which the works need to be accessed; (4) the types of users who want access; and (5) the barriers that currently exist or which are likely to exist in the near future preventing these users from obtaining access to the relevant copyrighted works.

Petitioners need not propose precise regulatory language or fully define the contours of an exemption class. Rather, a short, plain statement describing the nature of the activities the petitioners wish to engage in will be sufficient, as proponents will have the opportunity to further refine or expound upon their initial petitions during later phases of the rulemaking. The Office anticipates that in many cases petitioners will be able to adequately describe in plain terms the relevant information in a few sentences, or even a single sentence, as with the examples below.

Prof. Halderman is a computer scientist whose research focuses on computer security and privacy, with an emphasis on problems that broadly impact society and public policy, including software security, network security, data privacy, anonymity, electronic voting, censorship resistance, computer forensics, ethics, and cybercrime. He regularly conducts good faith security research on a variety of computer programs on devices and machines. These devices include voting machines, smartphones, and home routers, printers, and other "Internet of things" devices. He is especially well-positioned to speak to the ongoing necessity of renewing the current exemption for good faith security research on such devices because of his first-hand knowledge of the security research industry and his experience as an active participant in past triennial reviews for exemptions intended to mitigate the potential adverse effects resulting from legitimate security research. More specifically:

• In 2008, Prof. Halderman sought and received an exemption in connection with his non-infringing research into security flaws in digital rights management technologies included with sound recordings on compact discs.
• In 2010, Prof. Halderman sought and received an exemption in connection with his non-infringing research into security flaws in digital rights management technologies included with video games.
• In 2015, Prof. Halderman, in collaboration with several other security researchers, sought and received the existing exemption for security research.
• In 2018, Prof. Halderman advocated for the careful refinement and expansion of the existing exemption for security research to ensure that legitimate security research was encouraged and supported while continuing to mitigate the potential adverse effects of this research.

The Center for Democracy & Technology ("CDT") is a nonprofit public interest organization that supports laws, corporate policies, and technical tools to protect the civil liberties of Internet users and represents the public's interest in maintaining balanced copyright policies and a secure digital environment. CDT supports the clear and predictable application of laws and exemptions so that security researchers can perform beneficial research with certainty, and has advocated for a broad exemption to Section 1201's prohibition on the circumvention of technological protection measures in the 2015 and 2018 triennial rulemakings.

ACM (the Association for Computing Machinery) is the world's largest educational and scientific computing society. The ACM U.S. Technology Policy Committee (USTPC) serves as the focal point for ACM's interaction with the U.S. government in all matters of U.S. public policy related to information technology. USTPC's membership is comprised of individual computer scientists, educators, researchers, and other technology professionals. In the sixth triennial rulemaking, ACM's U.S. policy committee (renamed USTPC in 2018) strongly endorsed and documented the need for a new security research exemption to Section 1201 of the Digital Millennium Copyright Act (DMCA) in 2015 comments to the Copyright Office. Subsequently, in a 2017 filing in the last such proceeding, the Committee urged both renewal and expansion of that exemption. ACM first formally engaged with the Copyright Office on the matter of DMCA exemptions in February of 2000.

In addition to recommending and granting our July 22, 2020 petition to renew the temporary exemption for good-faith. Security research codified at 37 C.F.R. § 201.40(b)(7), Petition to Renew a Current Exemption Under 17 U.S.C. § 1201, Security Research – Halderman, CDT, ACM, (July 22, 2020), the above-referenced petitioners additionally ask the Office to modify and clarify that exemption.

Item B. Description of Proposed New Exemption *(cont'd)*

Good-faith security researchers aim to use their findings in positive ways to bolster academic publications and discussions of computer program and software security, to uncover security flaws and vulnerabilities and then alert consumers and notify companies of such concerns, and to develop new, secure versions of computer programs and software. Though the existing exemption is an important step in the direction of fostering this important type of good-faith security exploration, researchers who make use of it—and who would like to make use of it—find that its numerous caveats make it difficult to determine whether their respective work will fall under the protection of the exemption. These many caveats in the exemption make it less effective because they create risky uncertainty and chill legitimate, productive research.

It is for these reasons, and others, that petitioners request that the Office make the following severable modifications and clarifications to the existing exemption for good-faith security research:

(1) Remove the limitation that circumvention be undertaken 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" to avoid potentially importing the implications, obligations, penalties, and general uncertainty associated with other non-copyright legal regimes into copyright law through the security research exemption;

(2) Remove both references to the term "solely" from the provisions of the exemption in 37 C.F.R. § 201.40(b)(7)(i) and (ii) to avoid unconstitutionally limiting post-circumvention First-Amendment-protected speech that includes information derived from good-faith security research;

(3) Remove the limitation that "the 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" to avoid unconstitutionally limiting post-circumvention First-Amendment-protected speech that includes information derived from good-faith security research and to avoid conditioning security researchers' ability to circumvent in service of that speech on post-circumvention behavior by third parties whose behavior researchers do not control.

Petitioners recognize that many of these requests were considered by the Office in the prior rulemaking and were rejected—wrongly, in our view—on the grounds that the record was not adequately developed. We intend to further develop the record in favor of these changes in the current rulemaking period. These changes continue to be critical as security researchers face significant uncertainty as a result of individualized and often difficult legal analysis the exemption requires for new research projects. The complexity of this exemption and the related legal analysis continues to result in extensive chilling of security research.

This dynamic's implication of the First Amendment has also taken a new sense of urgency in light of the holding in Green v. DOJ, where the D.C. District Court acknowledged that "the DMCA and its triennial rulemaking process burden the use and dissemination of computer code, thereby implicating the First Amendment." 392 F. Supp. 3d 68, 86 (D.D.C. 2019). In other words, the triennial rulemaking process and resulting security research exemptions were identified as a central issue in Green because they implicate the First Amendment rights of security researchers whose speech is "[burdened] substantially more . . . than is necessary to further the government's legitimate interests." Id. at 95. The Office must, at a minimum, endeavor to address this conflict by making the requirements of the security research exemption, narrow, clear, and highly tailored to limit any unnecessary chilling effects.

The other underlying aspects of the exemption should remain the same or similar to those in the current temporary exemption. In particular:

(1)"[T]he types of copyrighted works that need to be accessed" continue to include computer programs of all types, and including associated literary, audiovisual, and other works;
(2) "[T]he physical media or devices on which the works are stored or the services through which the works are accessed" continue to include devices or machines capable of storing computer programs;
(3) "[T]he purposes for which the works need to be accessed" continue to include the discovery and mitigation of security flaws, the advancement of academic knowledge about security, public awareness of security and security flaws, national security, and First Amendment-protected speech on those topics;

Item B. Description of Proposed New Exemption *(cont'd)*

(4) "[T]he types of users who want access" continue to include security researchers, both professional and amateur, in a variety of academic, industry, hobbyist, and other contexts; and
(5) "[T]he barriers that currently exist or which are likely to exist in the near future preventing these users from obtaining access to the relevant copyrighted works" remain those that underpin the current exemption—namely, (a) uncertainty about the scope of Section 1201's built-in statutory exemptions related to security research and (b) uncertainty about the scope of the unwarranted limitations in the current exemption, which we request that the Office address.