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

Alex Rice
Chief Technology Officer
HackerOne Inc.
arice@hackerone.com

HackerOne Inc. ("HackerOne") is the market leading hacker-powered security platform, helping organizations find and fix critical vulnerabilities before they can be exploited. HackerOne is headquartered in San Francisco with offices in London, New York, the Netherlands, and Singapore.

ITEM B. PROPOSED CLASS ADDRESSED

Proposed Class 13: Computer Programs—Security Research

ITEM C. OVERVIEW

HackerOne submits this comment in support of the proposals to expand Proposed Class 13 (Computer Programs—Security Research), the current exemption permitting circumvention for purposes of good-faith security research. In particular, HackerOne agrees with Professor J. Alex Halderman that the current exemption is too restrictive and limits the scope and effectiveness of security research.[1] As summarized in the Notice of Proposed Rulemaking, Professor Halderman suggests removing:

(1) *Other Laws Limitation* – the requirement that circumvention be undertaken on a "lawfully acquired device or machine on which the computer program operates" and "not violate any applicable law";

(2) *Access Limitation* – both instances of the term "solely" (i.e., "solely for the purpose of good-faith security research" and "solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability"); and

[1] *See* J. Alex Halderman, et al., Petition for New Exemption Under 17 U.S.C. § 1201, *available at* https://www.copyright.gov/1201/2021/petitions/proposed/New%20Pet.%20-%20J.%20Alex%20Halderman%20et%20al.pdf.

(3) *Use Limitation* – the requirement that the information derived from the activity be 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."[2]

For the reasons set forth below, HackerOne agrees that Proposed Class 13 should be expanded.

I. Background: The Value of Independent Security Research

Security researchers go by many names – finders, hackers, pen testers, breakers, etc. – yet they all face a monumental task. We live in an era of stunning security failures and breakneck innovation. Bad actors can now easily obtain the tools they need to steal our most precious resource: our information – health records, financial data, and private communication between friends and family to name a few. The stakes could not be higher. Security is everyone's responsibility.

Enter the hackers. Hackers are here for good, to bring their intelligence and their grit to bear against our connected society's toughest challenges. We are at the forefront of a tectonic shift: rather than putting our collective safety in the hands of the few, the burden of our security is now shared by many.

Organizations like the Department of Defense, Goldman Sachs, Facebook, and Google have embraced hacking as part of a mature security infrastructure. To date, HackerOne has partnered with more than 1,700 customer programs to help find over 150,000 vulnerabilities and award more than $82 million in bug bounties.

As hacking grows in popularity, though, not all organizations welcome this positive security progress with a mindset of acceptance. Nearly two-thirds of hackers say they have found bugs and chosen not to report them to the organization. Thirty-eight percent of hackers said this was due to "threatening legal language" posted on the organization's website regarding the discovery of potential vulnerabilities. In other cases, 21% said the companies did not have an obvious channel through which to report findings, and another 15% said that the company was unresponsive to previous bug reports. That is thousands of bugs that have gone unreported, and a significant amount of untapped potential.

The U.S. federal government has a role to play in encouraging the use and growth of hacker-powered security. In particular, the U.S. Copyright Office should ensure its regulations – and, in this case, its exemptions under the Digital Millennium Copyright Act ("DMCA") – allow security researchers to do their jobs to the fullest extent possible.

II. Proposed Class 13 (Computer Programs—Security Research) is Too Restrictive

When deciding whether to grant a temporary exemption to the DMCA's prohibition against circumvention of technological measures that control access to copyrighted work, the U.S. Copyright Office must weigh statutory factors including, among others, "the impact the

[2] *See* Exemptions to Permit Circumvention of Access Controls on Copyrighted Works, 85 Fed. Reg. 65293, 65307 (Oct. 15, 2020).

prohibition on the circumvention of technological measures applied to copyrighted works has on . . . research."[3] While HackerOne applauds the U.S. Copyright Office for its intention to recommend each of the existing exemptions for readoption,[4] Proposed Class 13 (Computer Programs—Security Research) that permits circumvention for purposes of good-faith security research does not go far enough.

As noted above, Proposed Class 13 contains three limitations that restrict the scope and effectiveness of security research: (1) Other Laws Limitation; (2) Access Limitation; and (3) Use Limitation. Each should be removed for the reasons further articulated below.

(1) Other Laws Limitation

The Other Laws Limitation requires that circumvention be undertaken on a "lawfully acquired device or machine on which the computer program operates" and "not violate any applicable law."

With respect to the first requirement, it is sometimes difficult or impossible for researchers to "lawfully acquire" the hacked device or machine – for example, where software is provided as a service (e.g., Dropbox or Slack) and accessed through a website. In 2019/2020, HackerOne conducted a survey among 3,150 respondents from over 120 countries and territories ("Hacker Report").[5] When asked what is their favorite kind of platform or product to hack, 71% responded that they surface security flaws in websites.[6] Unfortunately, these researchers may not be able to find protection under Proposed Class 13 because they are not in lawful possession of the devices or machines that house the computer programs on which the websites are run. To ensure the exemption protects security researchers where they do the most good, this requirement should be removed.

With respect to the second requirement, HackerOne believes that the DMCA and its penalties thereunder should stand on their own and not be tied to penalties in other laws. In the security research space, laws governing ethical hacking are increasingly in flux. For example, the U.S. Supreme Court is set to interpret a key provision of the Computer Fraud and Abuse Act ("CFAA") in *Van Buren v. United States*. At issue is the definition of "exceeds authorized access" in relation to one intentionally accessing a computer system they have authorization to access. The exact definition is not clear and has created a 4-3 Circuit split. The Court's decision will not only have a significant impact on the defendant, who was found guilty of violating the CFAA and sentenced to 18 months in prison, but also on defendants in future CFAA prosecutions – where first-time offenses for accessing a protected computer without sufficient "authorization" can be punishable by up to five years in prison (ten years for repeat offenses), plus fines. Voiding an exemption under the DMCA for a violation of another law, like the

[3] *Id.* at 65294.

[4] *Id.* at 65293.

[5] *The 2020 Hacker Report*, HackerOne, *available at* https://www.hackerone.com/resources/reporting/the-2020-hacker-report [hereinafter "Hacker Report"].

[6] *Id.* at 32.

CFAA, only serves to compound already hash penalties without any further deterrent effect. Like the first requirement, it also should be removed.

(2) Access Limitation

The Access Limitation requires that the researcher circumvent "solely for the purpose of good-faith security research" and "solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability." As the Hacker Report uncovered, security researchers hack not just for testing, investigation, or correcting flaws or vulnerabilities, but for a host of other reasons too.[7] When asked why do they hack, more than two-thirds responded that they do so to be challenged, while half also do it to learn and contribute to the advancement of security knowledge. Importantly, what these security researchers uncover are then disclosed for remediation. So long as these security researchers do not take ill-advantage of the vulnerabilities they uncover, they should not be forced to hack *solely* for the enumerated reasons in order to claim the exemption's protection. The "solely" limitation should therefore be removed.

HackerOne agrees, though, that bad faith actors should not be able to hide behind this exemption. In addition to removing the "solely" limitation, we also urge the U.S. Copyright Office to further clarify what "good faith" security research means. The explanation contained in the Cybersecurity and Infrastructure Security Agency's ("CISA") Binding Operational Directive ("BOD") 20-01, requiring all federal agencies to develop and publish a vulnerability disclosure policy ("VDP"),[8] is instructive:

> "[G]ood faith" means security research conducted with the intent to follow an agency's VDP without malicious motive; your agency may evaluate an individual's intent on multiple bases, including by their actions, statements, and the results of their actions. In other words, good faith security research means accessing a computer or software solely for purpose of testing or investigating a security flaw or vulnerability and disclosing those findings in alignment with the VDP. The security researcher's actions should be consistent with an attempt to improve security and to avoid doing harm, either by unwarranted invasions of privacy or causing damage to property.[9]

(3) Use Limitation

Finally, the Use Limitation requires that the information derived from the activity be used "primarily to promote the security or safety of the class of devices or machines on which the

---

[7] *Id.* at 35.

[8] A vulnerability disclosure policy, or VDP, is an organization's formalized method for receiving vulnerability submissions from the outside world. A VDP is intended to give security researchers clear guidelines for reporting potentially unknown or harmful security vulnerabilities to the proper person or team responsible.

[9] *What Does the Directive Mean by "Good Faith"? - BOD 20-01*, CISA (Sep. 2, 2020), *available at* https://cyber.dhs.gov/bod/20-01/#what-does-the-directive-mean-by-good-faith. While CISA's definition of "good faith" includes the word "solely", its meaning takes a more holistic approach when read in conjunction with the second phrase in the sentence requiring "disclosing those findings" and the last sentence emphasizing the intent of the security researcher to "improve security and to avoid doing harm."

computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement." The idea behind security research is to identify vulnerabilities before bad actors can find them, and it is common for vulnerabilities to appear across devices. Moreover, in addition to finding and reporting a vulnerability to that device's owner, a security researcher should be able to share his or her findings with others.

In short, transparency should not have consequences.

The Use Limitation, though, discourages security researchers from sharing their results by preventing a researcher from claiming the exemption if a bad actor takes advantage of that researcher's vulnerability announcement. To encourage the sharing of information, the Use Limitation should be removed.

III. Conclusion

Those who call themselves "security researchers" are on the rise. Hundreds of hackers are registering to join the ranks every day – nearly 850 on average – and their numbers have doubled in the past year to more than 800,000 registered individuals on the HackerOne platform alone.[10] The contributions of this community are now a fundamental driver of holistic improvements to cybersecurity. It is important that the U.S. government work to ensure that its policies and regulations (and, here, exemptions) do not stifle this growth.

The three limitations in Proposed Class 13 (Computer Programs—Security Research) send the message that only very particular types of good faith security research will be protected from the DMCA's prohibition against circumvention of technological measures that control access to copyrighted work. For the above reasons, these limitations should be removed.

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

N/A

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

See response in Item C.

DOCUMENTARY EVIDENCE

N/A

[10] *Id.*