💬 **PUBLIC SUBMISSION**

Comment from A group of hackers at DEF CON

Posted by the **U.S. Copyright Office** on Aug 14, 2023

View More Comments (40) (/document/COLC-2023-0004-0002/comment)

View Related Comments (40) (/docket/COLC-2023-0004/comments)

Share ⌄

Comment

We are a group of more than a dozen security and policy professionals attending the DEF CON 31 security conference. We have diverse experience and expertise in the security research space, representing both public and private sectors. We write in support of the Blaze and Bellovin petition to renew the security research exemption to DMCA Section 1201.

We can confirm that the need for this exemption from DMCA Section 1201 continues to be present. Among our group are individuals who conduct security assessments on software for which they do not own the copyright. Our experience is that this kind of good faith security research creates an expectation in software vendors that their software will be tested for security, which incentivizes them to develop more resilient software. This advances the security of the software, systems, and users of that software in a way that benefits the public. Our experience is that copyright is not undermined by good faith security research.

We can confirm that the security testing exemption has led to additional creative works, such as the creation of software to fix vulnerabilities, as well as papers and presentations on security research. This exemption (following several iterations) has helped cultivate an expectation between software vendors and researchers, and has helped establish relationships and a creative ecosystem upon which the livelihoods of many security professionals depend. If this exception were not to be renewed, not only would these creative works be disrupted, there would be a loss of essential efficiencies and resources that help advance security.

Just this week, as part of the research activities conducted at DEFCON 31, security researchers have worked collectively to advance security of users and society by conducting research that may include circumvention of protection measures of copyrighted works, code, that has resulted in the identification of vulnerabilities. These activities include research of numerous types of devices such as connected cars, IoT devices, medical devices, devices deployed across critical infrastructure, and more.

Recently we have seen the Administration, as well as other policymakers globally, advance requirements and best practices that include coordinated vulnerability disclosure and the ability to receive reports of

vulnerabilities submitted from unsolicited sources.These include, the IoT Cybersecurity Improvement Act, NISTIR 800-213A, the Administration's encouragement of AI red teaming activities, among others. The adoption of this petition is consistent with this approach of recognizing the value of good faith security research to advance security.

Our support of this petition should not be construed as opposition to an expanded exemption for security testing under DMCA Section 1201. There continues to be a need for an expanded, more flexible exemption to enable good faith security research to advance the security of users, systems, and devices in other contexts.

We are encouraged by the Copyright Office's continued effort to extend and advance the broader interests of society and protection of users, as evident by the security research exemption. As the Copyright Office continues to evolve its thinking around this effort, the security community would be delighted to serve as a resource and engage with the Copyright Office. The security of the nation is a critical priority we must collectively strive to advance.

Respectfully,
A group of hackers at DEF CON

Comment ID
COLC-2023-0004-0041

Tracking Number
ll7-8efl-u7ku

Comment Details	Submitter Info

Organization Name
A group of hackers at DEF CON