

Docket (/docket/COLC-2017-0007) / Document (COLC-2017-0007-0070) (/document/COLC-2017-0007-0070)
/ Comment

 PUBLIC SUBMISSION

Class_10_InitialComments_Rapid7 et al.

Posted by the **U.S. Copyright Office** on Dec 19, 2017

View More Comments 181 (/document/COLC-2017-0007-0070/comment)

View Related Comments 249 (/docket/COLC-2017-0007/comments)

Share ▾

Comment

Short Comment to US Copyright Office
Seventh Triennial Section 1201 Proceeding (2018)
Class 10: Computer Programs Security Research

Dec. 18, 2017

The undersigned cybersecurity companies support renewal of the current exemption for good faith security research at 37 CFR 201.40(b)(7). In addition, the undersigned wish to express support for two critical modifications recommended in the Class 10 petitions of Felten & Halderman and the Center for Democracy & Technology (CDT) to expand the current exemption.

1) Removal of the requirement that circumvention "not violate any applicable law, [including] the Computer Fraud and Abuse Act." [See CDT Class 10 Pet. at 2, recommendation #3; Felten & Halderman Class 10 Pet. at 2, recommendation #2.]

The security testing exemption does not void compliance with any other laws outside 17 USC 1201, but the exemption should not be contingent on compliance with all other laws. Violations of other laws carry their own penalties, remedies, and enforcement mechanisms separate from copyright and the Librarian of Congress. As the Register noted in 2015, "the rules that should govern [security research] are best considered by those responsible for our national security and for regulating the consumer products and services at issue." Security research can implicate numerous federal and state regulations, with legal uncertainty and uneven application in different jurisdictions. For example, state laws vary considerably, can change quickly, are often ambiguous, and may prohibit conduct otherwise permissible under the security testing exemption. Another example: The extent to which a violation of terms of service is punishable under the CFAA is subject to split interpretations in US courts, leading to unclear liability. [See US v. Nosal, 828 F.3d 865 (9th Cir. 2016); US v. Valle, No. 14-2710 (2d Cir. 2015)] Yet if an act of research violates CFAA, the researcher could be sued privately or prosecuted criminally under CFAA. [See 18 USC 1030(c), (g)]

Voiding the Sec. 1201 exemption due to a CFAA violation would only have the effect of compounding penalties that are already strict under CFAA. To achieve the goal of the Sec. 1201 exemption and avoid chilling good faith security research, the exemption should provide a clear safe harbor under copyright law, rather than requiring researchers to navigate large bodies of unsettled law and complex jurisdictional issues, with potentially severe penalties for missteps.

2) Removal of the requirement that "the information derived from the activity is [...] not used or maintained in a manner that facilitates copyright infringement." [See CDT Pet. at 2, recommendation #7, Felten & Halderman Pet. at 2, recommendation #5.]

A security testing exemption to Sec. 1201 should not penalize researchers for unintended third party uses of research results. Good faith security research does not seek to infringe copyright. Instead, the end goals of security research are typically to promote transparency of cybersecurity vulnerabilities that put consumers and businesses at risk, ideally prompting a patch or correction to the vulnerability. To achieve these goals, it is common practice for security researchers to disclose the results of research publicly, including through the NIST National Vulnerability Database (NVD) and Common Vulnerabilities and Exposures (CVE) index of publicly known cybersecurity vulnerabilities. Though the purpose of public disclosure and NVD/CVE is generally to prevent vulnerability exploitation by raising awareness and encouraging fixes, it is also possible for malicious actors to exploit known vulnerabilities. If a malicious actor exploits a known vulnerability for the purpose of violating copyright (such as by stealing copyrighted material from another computer), the researcher that discovered or publicly disclosed the vulnerability ("the information derived from research") should not be considered to have "facilitated copyright infringement." To avoid this scenario, the exemption language could be removed or possibly modified to read "where the information derived from the activity [...] is not primarily used or maintained for the purpose of facilitating copyright infringement." This modification should help protect security testing information disclosed publicly for cybersecurity purposes, but exclude security testing information disclosed to enable infringement.

Thank you for considering our recommendations.

- Rapid7
- Bugcrowd
- Duo Security
- HackerOne
- Luta Security

Comment ID

COLC-2017-0007-0095



Tracking Number

1k1-90fa-j723

Comment Details

Submitter Info

Submitter Name

Harley Geiger

Organization Name

Rapid7 et al.



Your Voice In Federal Decision Making

[About \(/about\)](#) [Agencies \(/agencies\)](#) [Learn \(/learn\)](#)

[Reports \(https://resources.regulations.gov/public/component/main?main=Reports\)](https://resources.regulations.gov/public/component/main?main=Reports) [FAQ \(/faq\)](#)

[Privacy & Security Notice \(/privacy-notice\)](#) | [User Notice \(/user-notice\)](#) | [Accessibility Statement \(/accessibility\)](#) | [Developers \(https://open.gsa.gov/api/regulationsgov/\)](https://open.gsa.gov/api/regulationsgov/)

[Support \(/support\)](#) [Provide Site Feedback](#)