

*This is a Word document that allows users to type into the spaces below. The comment may be single-spaced, but should be in at least 12-point type. The italicized instructions on this template may be deleted.*

UNITED STATES COPYRIGHT OFFICE



**Long Comment Regarding a Proposed  
Exemption Under 17 U.S.C. § 1201**

**Comments of ACT| The App Association on Proposed Class 10: Computer  
Programs- Security Research**

**ITEM A. COMMENTER INFORMATION**

ACT | The App Association  
Morgan Reed  
President  
1401 K Street, NW  
Suite 501  
Washington, District of Columbia 20005  
(202) 331-2130  
[mreed@actonline.org](mailto:mreed@actonline.org)

ACT | The App Association, representing more than 5,000 app companies and software firms that create and license digital content, submits the following comments to the United States Copyright Office (“Copyright Office”) in response to its Notice of Proposed Rulemaking (“NPR”) concerning possible temporary exemptions to the Digital Millennium Copyright Act’s (“DMCA”) prohibition against the circumvention of technological measures that control access to copyrighted works. The App Association is widely recognized as the foremost authority on the \$143 billion app ecosystem and its intersection with governmental interests. As the only organization dedicated to the needs of small business app developers and tech innovators around the world, the App Association advocates for an environment that inspires and rewards innovation while providing the resources to help our members leverage their intellectual assets to raise capital, create jobs, and support innovation.

**Privacy Act Advisory Statement:** Required by the Privacy Act of 1974 (P.L. 93-579)

The authority for requesting this information is 17 U.S.C. §§ 1201(a)(1) and 705. Furnishing the requested information is voluntary. The principal use of the requested information is publication on the Copyright Office Web site and use by Copyright Office staff for purposes of the rulemaking proceeding conducted under 17 U.S.C. § 1201(a)(1). NOTE: No other advisory statement will be given in connection with this submission. Please keep this statement and refer to it if we communicate with you regarding this submission.

## **ITEM B. PROPOSED CLASS ADDRESSED**

Class 10-Computer programs- Security Research

## **ITEM C. OVERVIEW**

ACT | The App Association opposes the proposed class 10 exemptions that remove the specific security research categories and limitations. App Association members understand the important role of security research in the mobile app industry. However, petitioners have not established that they are or are likely to be harmed in their ability to make non-infringing uses of copyrighted works because of the prohibition on circumvention without the removal of the limitations on the current exemption for security research. The exponential growth in the mobile app economy is proof that the system is working. The safety valves intended to balance copyright rights with the public interest in the DMCA work. Developers continue to innovate and consumers have access to a wide range of products and services in a variety of business models. Granting these requests would diminish app developers' incentive to innovate, and create challenges to their ability to monetize products, provide customer service, protect data, and comply with licensing agreements.

## **ITEM D. COMMENTS**

Security research on computer programs is an important and necessary part of innovating software products and services that meet the needs of consumers. The DMCA includes security research as one of 10 exemptions to the prohibition on circumvention. In fact, Congress limited its scope of exemptions when it recognized the risk a broad exemption posed to the effectiveness of the copyright protections. Specifically, Congress limited acts of circumvention for security testing to "good faith testing" with the authorization of the copyright owner. In its 2015 Rulemaking, the Copyright Office determined that because the security research, encryption, and reverse engineering exemptions in the DMCA did not "permit the full range of legitimate security research" a temporary exemption was granted for computer programs that operate devices and machines for purposes of "good faith" security research. The Copyright Office should renew the 2015 exemption without modification. It strikes the appropriate balance between the need for important security research and necessary protections for digital copyrighted works.

Petitioners argue that the “good-faith” limitation is a two-pronged access limitation that prevents “scientific dialogue, academic peer review, and classroom teaching.” Petitioners claim the requirements that security testing be done “*solely* for the purpose of good-faith testing” (emphasis added) and the limitation that “the information derived from the activity is used *primarily* to promote the security or safety” (emphasis added) of the class of devices or machines or those who use them are ambiguous and create a chilling effect on research because of the potential they create for litigation. However, comments filed by the Center for Democracy & Technology (CDT) list specific recent examples of published results from security research on automotive security, medical devices, voting systems, and consumer devices, which challenge the oft-repeated claim of chilling effects on research and education.

Underlying the petitioners’ request for the removal of these exemptions is essentially a request for rights to access any software on any consumer device. Petitioners claim that the limitation in the 2015 exemption for computer programs that “operate devices and machines primarily designed for use by individual consumers” is also unclear and results in reluctance to engage in research on certain devices and systems. Petitioners support their request by focusing on the concerns for privacy and safety of consumers. These concerns are not among the factors the Copyright Office must consider in determining whether users are adversely affected in their ability to make non-infringing uses of copyrighted works protected by technological protection measures (“TPMs”). The response to concerns over what devices are included in the exemption is to not remove the limitation entirely. In its NPR, the Copyright Office reiterates the legislative history of the DMCA instructs that exempted classes should “be a narrow and focused subset of the broad category of works.” This request would essentially expose all software on any device to unauthorized access for any purpose. The App Association urges the Copyright Office to deny this request.

The App Association strongly supports maintaining the limitations on the current security research exemption. The practices of security research, encryption research, and reverse engineering must be balanced with the need to adequately maintain the integrity of software using TPMs like authentication and encryption. The use of TPMs is crucial to maintaining the integrity of software, protecting end-user data collected by consumer

products with embedded software from nefarious actors, and upholding the obligation to protect end-users' privacy rights.

Since the DMCA came into effect, the courts have provided further clarity around these exemptions that have provided increased certainty for copyright holders and the public (*e.g.*, *Davidson & Associates v. Jung*). The App Association discourages sweeping changes to copyright law based on theoretical legal arguments and speculative harms.

The DMCA was enacted to give incentives to creators and innovators to enter the digital marketplace. It accomplished this goal and continues to provide mobile app developers with the ability to protect their software from unlawful access. The explosive growth in the app ecosystem, and the wide range of businesses it supports, would not be possible without the protections, incentives, and security research provisions of the DMCA.

The petitioners have not established that they are or are likely to be harmed in their ability to make non-infringing uses of computer programs without the requested exemption. There simply isn't a problem to solve. Therefore, the App Association urges the Copyright Office to reject the petitioners' requests to remove categories and limitations from the exemption for security research as adopted in the 2015 rulemaking procedure.