*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 13: 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

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 $1.7 trillion 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 drive innovation.

### ITEM B. PROPOSED CLASS ADDRESSED

Class 13: Computer Programs - Security Research

## ITEM C. OVERVIEW

Security research is a critical and necessary part of innovation in digital products and services. App Association members regularly engage in legitimate security research as software developers and business owners. Security testing on computer programs is a routine step in the process of innovating software products and services that meet the needs of consumers.

The growth in the mobile app economy is proof that the system is working. The intent of the safety valves in the Digital Millennium Copyright Act (DMCA) is to balance the interests of rightsholders with the public interest in access to copyright work. The petitioners propose, again, a security research exemption that essentially removes all limitations to circumvent the technological protection measures (TPMs) used by innovative software developers to protect the safety, integrity, and functionality of their products and services. However, petitioners have failed to develop the record since the 2018 rulemaking by not providing more than *de minimus* evidence that they are, or are likely to be, harmed in their ability to make non-infringing uses of computer programs and embedded software because of the prohibition on circumvention. The requested exemption would diminish app developers' incentives to innovate and create challenges to their ability to monetize products, provide customer service, protect data, and comply with licensing agreements.

## ITEM E. ASSERTED ADVERSE EFFECTS ON NON-INFRINGING USES

The App Association opposes the proposals to remove the limitations in the current exemption that require performing security research on lawfully acquired devices "solely" for the purpose of good-faith research, does not violate any applicable law, and that information from the activity be used primarily to promote the safety of the device or machine on which the computer program operates. The same proposals were submitted in the 2018 rulemaking. The Registrar did not recommend removal of the limitations then and should reject them again in this rulemaking because the proponents have failed to demonstrate that without the changes they are, or are likely to be, adversely effected in their ability undertake non-infringing security research.

1. The Petitioners for Proposed Class 13 failed to meet the standard for granting an exemption.

The limitation that eligibility for the security testing exemption, under the statutory exemption in Section 1201(j) of the DMCA and the current temporary exemption, is available only when done on a "lawfully acquired device or machine" and not violate "any applicable law" strikes the appropriate balance, and petitioners have not proven actual harm to justify their removal. The petitioners claim these restrictions are ambiguous and create additional legal risks. In 2018, the Registrar recommended language for the current exemption to address situations in which a researcher is not able to "acquire" physical possession of the work. The Final Rule removed the device limitation to allow circumvention for situations involving websites and software provided as a service. Congress specifically included the requirement that researchers must also comply with other laws in Section 1201. Petitioners can only refer to this as a "potential cause of action" that expands the scope of 1201. The concern is unfounded since the research would need to be

willfully in violation of Section 1201 and for the purpose of commercial advantage or private financial gain in order to be criminally liable.

The requirements to perform security testing "solely" for good-faith research and that the information be used "primarily to promote the security or safety of the class of device or machine" did not have a chilling effect on researchers in this area. Professor Halderman claims that the term "solely" is ambiguous, and therefore, "All aspects of security research, from scholarship, teaching, and testing, to commenting, criticizing, and reporting, are disincentivized by the limitations and ambiguities in the current exemption." That claim does not comport with the evidence of a vibrant security testing marketplace. On October 20, 2020, *GlobalNewswire* posted an article titled, "Global Security Testing Market Expected to Surpass $27,593.9 Million by 2027." The article focused on how the growing prominence of cloud-based security testing and modern technologies would create huge opportunities for the security testing marketplace. The Software Freedom Conservancy expressed concerns that because privacy-focused research is beyond the scope of the exemptions in Sections 1201(j) and 1201(i) privacy research is unprotected. Temporary exemptions to 1201 need to be based on actual harms and not just theoretical. The reality is consumers can choose the ecosystem that works best for them as both closed and open-source systems are flourishing. Customized networks tailored to personal needs and desires can be built by the novice consumer to the advanced technology expert.

Private industry has welcomed the assistance of hackers, researchers, and security testers through "bug bounty" programs. A bug bounty program is a deal offered by many websites, organizations, and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities. On September 16, 2020, *Digital Privacy News* published an article titled, "The Security Flaw That Almost Knocked Apple Off Its Perch." The article detailed how Apple's bug bounty program resulted in a $100,000 payout for a hacker who discovered a flaw in the "Sign in With Apple" feature and that Microsoft had paid out $13.7 million in bug bounties over the past year to more than 300 hunters. Graham Dufault, senior director for public policy at the App Association, stated in the article that "Bug-bounty programs are likely becoming an important best practice for a widening swath of industries." Implementation of vulnerability disclosure practices occur after considerable due diligence by most companies and businesses because of litigation risks. The petitioners' proposed new exemption for security testing would undermine private industry options to employ hackers as a means of improving the safety and reliability of their products.

The proposed exemption also leaves out the limitation that an exemption for security research must not facilitate copyright infringement. This limitation is essential, and the App Association strongly supports preserving it in the renewal of the current exemption.

2. Removal of the limitations in the statute and existing exemption will harm the software marketplace.

The current limitations on the security research exemption are critical to the continued success of the software and mobile app industry. The practices of security testing, encryption research, and reverse engineering must find a balance with the need to adequately maintain the integrity of software using TPMs like authentication and encryption. The proposed new exemption for security testing effectively removes all protections afforded to software developers to protect their code, their business, and their customers.

Innovative app developers rely on firmware TPMs like authentication and encryption to allow legitimate uses of works and mitigate serious threats to user privacy. The use of digital rights management tools (DRM) or TPMs is critical to protection against unauthorized access to the copyright protected software but also against attempts to steal personal information. In fact, digital products and services developed for every industry must comply with federal, state, and international privacy laws to protect consumer privacy. The Children's Online Privacy Protection Act (COPPA), the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act, the California Consumer Privacy Act (CCPA), and the EU's General Data Protection Regulation (GDPR) are just some of the laws requiring tech developers to use technical means, including encryption, to protect consumer information. This technical protection, whether used for DRM or privacy, has the same underpinning. It is impossible to isolate the issue of whether to expand DMCA exemptions to only the copyright concerns. The vast personal information accessed through the mobile apps on smartphones, websites, and connected devices and machines must be protected according to these laws.

TPMs protect layers of licensed software in devices. Licensed software is part of most products with digital content embedded in them. The system of licensed software is a crucial component to the investment and distribution in existing products and future innovations. The benefits to consumers across a wide variety of products and services at every price point cannot be understated. It also allows software competitors access to product codes, which is a disincentive to innovation. Fortunately, there are alternative options to address many of the concerns expressed regarding access to software. Notices to consumers about restrictions and allowable uses along with offering certified third-party repair services can protect consumers and software developers. App Association members and those of other content and tech industries rely on licensed software to continue to offer low-cost, consumer friendly products across a growing range of business models.