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 11: Computer Programs - "Jailbreaking"

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

Proposed Class 11: Computer Programs -"Jailbreaking"

ITEM C. OVERVIEW

The App Association opposes the proposed new class 11 exemption for “routers and other networking devices” and the request to clarify the current exemption includes “non-integrated streaming devices.” The proponents of the proposed exemption did not provide sufficient rationale to meet the standard necessary to grant the expansion of the current exemption to include these devices. In addition, the proposed inclusion of all devices capable of transmitting video to televisions is overbroad and would negatively impact the market for mobile software applications and expose consumers to harm. The proponents’ evidence and arguments fail to acknowledge the real intent behind the exemption, which is to gain free access to all movies and television programs. Proponents completely ignore the well-documented risks to consumers who jailbreak their devices. This proposed exemption is an attempt to continue chipping away at the ability of creators and innovators to protect their intellectual property. Innovation in spite of past exemptions for jailbreaking of different devices does not simply mean the same will be true for streaming devices. Content streaming increased significantly in recent years, as has streaming piracy. This exemption will put content creators at a disadvantage in the constant challenge to stay one step ahead of infringing technologies. Content and software developers will face additional challenges and costs in bringing a variety of low-cost digital products and services to consumers. The potential harms far outweigh the claimed adverse or *de minimus* impacts on non-infringing uses of these devices.

ITEM D. COMMENTS IN OPPOSITION OF PROPOSED CLASS 11 EXEMPTION

1. The proponents for Proposed Class 11 fail to meet the standard required to grant an exemption because the proposed uses of the device software do not qualify as fair use.

In the NPR, the Copyright Office sets the standard for granting a temporary exemption from the prohibition on DMCA-dictated circumvention. The DMCA allows exemptions when “persons who are users of a copyrighted work are, or are likely to be in the succeeding three year period adversely affected by the prohibition… in their ability to make non-infringing uses under [title 17] of a particular class of copyrighted works.” The proponents’ petition for a new exemption and a clarification of the existing exemption fails to meet the standard for non-infringing uses and provide little evidence to support the claim they are being adversely affected by the prohibition on circumvention.

Software is a literary work and eligible for copyright protection under Section 102 of the Copyright Act. The Copyright Office stated in its Circular 1, *Copyright Basics*, section “What Works Are Protected,” that “Copyright, a form of intellectual property law, protects original works of authorship including literary, dramatic, musical, and artistic works, such as poetry, novels, movies, songs, computer software, and architecture.” Firmware, a type of software developed for use in devices to ensure that they operate as the manufacturer intended, is eligible for copyright protection. The Copyright Office’s recommendations for circumvention exemptions to firmware, adopted by the Librarian of Congress, in the last three rulemaking proceedings support that conclusion.

Circumvention of technological protection measures ("TPMs") of computer programs on a "lawfully acquired router or networking device on which the computer program operates" is an infringing activity. The DMCA gave creators and innovators the right to control access to their works with digital locks to encourage distribution of digital products and services that would in turn benefit the public. The petitioner states that the purpose, or intended use, of these computer programs is to install alternative firmware, upgrade software, fix security flaws, and enable new functionality. However, the petitioner did not submit evidence for the record to demonstrate the intent to use the exemption to install lawfully acquired software in order to be covered by fair use. Another factor in the fair use analysis is the impact of the use on the marketplace. There is a wide variety of options when it comes to selecting routers and networking systems. While proprietary firmware and computer programs are used by some manufacturers, there are extensive open-source options available. Hobbyists and tinkerers can utilize these options to personalize their networks without having to circumvent copyright-protected software that could negatively impact the market for those works.

Same as the request for a router exemption, the purposes for which the petitioners claim to want to use the software on streaming devices do not constitute a fair use. Case law and the record created by the Copyright Office in previous rulemaking proceedings focuses on the "purpose" or "intent" of the user when applying the fair use factors. Petitioners state the desire to use the firmware or device software to "display additional channel information," "replace the home screens," "take greater control of their privacy," and "connect the device with other personal devices." Yet, an internet search request for "Why should I jailbreak my streaming device?" reveals that the primary reason people want to jailbreak these devices has nothing to do with the reasons provided by the petitioner.

What is "jailbreaking"? According to an article published on www.kaspersky.com on November 6, 2020, jailbreaking "…is the process of exploiting the flaws of a locked-down electronic device to install software other than what the manufacturer has made available for that device." But, in a February 1, 2021, post on www.firesticktricks.com, jailbreaking was described as "…a simple process of unlocking your FireStick [sic] and allowing yourself access to the bottomless pool of content on the internet." On January 19, 2021, https://troypoint.com had a similar post titled "How to Jailbreak Roku - Secret Method for Streaming Movies and Shows." In fact, this is the primary definition or purpose for jailbreaking a streaming device found on the internet. The petitioners wish to define jailbreaking as a colloquial term to install or remove some software on a device. The definition, however, according to most advocates for jailbreaking is more focused on how consumers unlock free content.

Fair use is determined after a four-factor analysis: 1) the purpose and character of the use; 2) the nature of the copyrighted work; 3) the amount and substantiality of the portion used; and 4) the effect on the market for the copyrighted work. Jailbreaking video streaming devices does not meet the standards set in case law and by the Copyright Office in rulemakings to qualify as a non-infringing use. Petitioners cite several cases where courts have found a fair use with respect to firmware. However, under each factor the decision has hinged on the purpose for the use—research, interoperability, or competition in the marketplace. In *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d (2004), the court found a fair use where the user was not seeking to unjustly benefit from the creative investment of writing the program code. *Sega v. Accolade*, 977 F.2d 1510 (9th Cir. 1992), the court found that research into software functionality weighed in favor of fair use. And in *Sony Computer Entertainment v. Connectix Corp.*, 203 F.3d 596 (2000), the Ninth Circuit again found fair use where reverse-engineering was done to create new interoperable games. The App Association supports findings of fair use for these purposes. The existing exemptions in the DMCA for security research, interoperability, and reverse engineering are extremely valuable tools to continued innovation in the mobile app industry. But that is not what is happening with respect to jailbreaking of streaming devices. The "why jailbreak?" search resulted in post after post focused exclusively on how to get free content. A www.wirefly.com post explained that most Roku users want access to the Kodi app and provided instructions on how to use virtual private networks (VPNs) to avoid detection from streaming pirate content readily available on it. The firesticktricks.com post summed it best when the author explained, "The answer to the question is rather simple. You jailbreak your Firestick [sic] to enjoy unlimited/free streaming without having to burn a hole in your pocket."

The App Association urges the Copyright Office to reject the claim that the intended use of firmware in routers and non-integrated streaming devices constitutes a non-infringing use in its analysis of the proposed jailbreaking exemption from the prohibition on circumvention.

2. The Proposed Class 11 exemption for jailbreaking is not narrowly defined and would harm the mobile app ecosystem.

In the NPR, the Copyright Office states that in evaluating the evidence presented with respect to a proposed exemption, it must consider "the effect of circumvention of technological measures on the market for or value of copyrighted works; …" Granting the proposed new exemption for routers and non-integrated streaming devices will negatively impact the ability of app developers to successfully compete in the digital streaming marketplace as both creators of firmware and applications that provide licensed content.

Like many other industries, the app industry experiences significant loss of revenue each year from piracy and counterfeits. Piracy presents a major threat to the success of App Association members and the billions of consumers who rely on digital products and services. Piracy—whether originating within the United States or abroad—threatens the creators of digital content by undermining their ability to innovate, invest, and hire. App developers have been at the forefront of technological innovations providing consumers with a variety of entertainment options in a range of price points. And with the rise of video streaming, app developers have been integral to the success of developing new content delivery platforms as well as streaming services. With the rise of streaming video, piracy of streamed content has also increased. In a 2019 report, "Impacts of Digital Video Piracy on the U.S. Economy," the U.S. Chamber of Commerce's Global Innovation Policy Center estimates that 80 percent of piracy is attributable to streaming and that global online piracy costs the U.S. economy at least $2.9 billion in lost revenue each year. As evidenced by the countless online posts and tutorials about how to jailbreak streaming devices in order to get free access to unlimited video content, granting an exemption permitting circumvention of TPMs used to protect the firmware on these devices would only exacerbate the piracy problem and lead to increased losses for mobile app developers.

It is important to understand the app ecosystem and the reason for its success to see how the DMCA protections have played a critical role. In nearly a decade of existence, the app ecosystem grew exponentially alongside the rise of the smartphone. Valued at $1.7 trillion, the app economy is driven by app developers and innovators who depend on software platforms to reach consumers around the globe. In 2018, the total number of app downloads was 194 billion (up from 178 billion in 2017), and the reach of software applications continues to grow.

The single most important factor in the app ecosystem's dynamic growth and unrivaled success is the presence of curated platforms (e.g., Apple's App Store, Google Play for mobile, Steam for games). Trusted app stores serve as a vital foundation for the growing uses of apps across industries and enterprises. Non-integrated streaming devices are simply extensions of the platform services and curated content delivery. Jailbreaking these devices to gain free access to content from unapproved apps threatens the market for App Association members innovating new means of developing and delivering content to consumers.

The market for firmware or embedded software to operate devices is thriving and essential to support the continued success of the platform content delivery model. In a June 14, 2019, post on www.electronicspecifier.com, the global embedded software market was predicted to grow to over $20 billion by 2025. App Association members compete in the firmware marketplace. The potential harm to this industry should not be discounted based solely on the Electronic Frontier Foundation's claims that "firmware is sold along with the devices themselves" and "jailbreaking has not harmed sales of similar devices." Firmware is a competitive market and firmware upgrades do not happen without additional costs of research, writing code, and testing. The App Association encourages the Copyright Office to learn more about the firmware marketplace before assuming that adopting the proposed new exemption for routers and non-integrated streaming devices would not have a negative impact.

3. The Proposed Class 11 exemption for jailbreaking will expose consumers to data security breaches, malware, malfunctioning devices, loss of product warranties, and potential criminal and civil litigation resulting from illegally streaming video content.

The DMCA allows app developers to protect their products and consumers. The use of TPMs is critical to protection against unauthorized access to a copyrighted work but also to protect consumers from harm. Piracy creates the potential for consumers to be victims of illegal sellers who pose as legitimate content owners or distributors. Counterfeit software apps can lead to customer data loss, interruption of service, malfunctioning devices, and even civil and criminal prosecution for copyright infringement.

Jailbreaking streaming devices, or any device, comes with a significant risk to the device owners. Petitioners claim that a primary purpose for jailbreaking is to allow users to take greater control over their privacy. However, in nearly every "how to" jailbreak article and post online, consumers are warned of the significant risks of jailbreaking a device, many of which stem from the fact that jailbroken devices defeat the ability of platforms to ubiquitously update devices' functionality and security, putting end user privacy at risk. In the www.kaspersky.com article, the disadvantages to jailbreaking include no more automatic updates, inability to apply some software updates, voiding the device warranty, losing access to content, and device failure. Another blog, from TDS Telecom, did a post titled, " 'Jailbroken' streaming devices and apps are Trojan Horses for Malware" on May 8, 2019. The post describes how purchasers of jailbroken devices think that they are getting free access to movies and TV but instead are exposing all their personal data, app information, and passwords to scammers. Most of the websites providing tutorials also warn users that the content owners, ISPs, and device makers use digital rights management tools and TPMs to monitor for illegal streaming. To avoid detection, the tutorials include steps to install VPNs to allow detection free streaming. This seems to be the primary privacy goal of jailbreaking streaming devices. For the causal consumer purchasing a jailbroken device or performing a jailbreak themselves, there is a risk of criminal and civil litigation for copyright infringement. Authorizing an exemption for this behavior will throw open the door to increased risk to the vast majority of consumers to be victims of fraud, or worse.

App Association members have a strong interest in protecting their customers. Piracy and counterfeit software apps threaten end-user confidence and can lead to customer data loss, interruption of service, revenue loss, and reputational damage. These threats have caused significant damage, and continue to pose substantial hazards, to app developers. It is essential that copyright owners be able to utilize encryption and other forms of access controls to combat these threats, which will be undermined by an exemption for jailbreaking routers and non-integrated streaming devices. The App Association strongly opposes the proposed new exemption and clarification for jailbreaking.