UNITED STATES COPYRIGHT OFFICE

Petition to Renew a Current Exemption Under 17 U.S.C. § 1201

8th Triennial Rulemaking

Please submit a separate petition for each current exemption for which renewal is sought.

NOTE: Use this form if you want to renew a current exemption without modification. If you are seeking to engage in activities not currently permitted by an existing exemption, including those that would require the expansion of a current exemption, you must submit a petition for a new exemption using the form available at **https://www.copyright.gov/1201/2021/new-petition.pdf**.

If you are seeking to expand a current exemption, we recommend that you submit both a petition to renew the current exemption without modification using this form, and, separately, a petition for a new exemption that identifies the current exemption, and addresses only those issues relevant to the proposed expansion of that exemption.

Item A. Petitioners and Contact Information

Please identify the petitioners and provide a means to contact the petitioners and/or their representatives, if any. The "petitioner" is the individual or entity seeking renewal.

Kit Walsh
Electronic Frontier Foundation
815 Eddy Street
San Francisco, California 94109
kit@eff.org

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 website and use by Copyright Office staff for purposes of the rulemaking proceeding conducted pursuant to 17 U.S.C. § 1201(a)(1). NOTE: No other advisory statement will be given in connection with this application. Please keep this statement and refer to it if we communicate with you regarding this petition.

Item B. Identify Which Current Exemption Petitioners Seek to Renew

Check the appropriate box below that corresponds with the current temporary exemption (see **37 C.F.R. § 201.40**) the petitioners seek to renew. Please check only one box. If renewal of more than one exemption is sought, a separate petition must be submitted for each one.

Motion Pictures *(including television programs and videos)***:**

- ○ Excerpts for educational purposes by college and university or K-12 faculty and students
- ○ Excerpts for educational purposes by faculty in massive open online courses ("MOOCs")
- ○ Excerpts for educational purposes in digital and literacy programs offered by libraries, museums, and other nonprofits
- ○ Excerpts for use in nonfiction multimedia e-books
- ○ Excerpts for use in documentary filmmaking or other films where use is in parody or for a biographical or historically significant nature
- ○ Excerpts for use in noncommercial videos
- ○ For the provision of captioning and/or audio description by disability services offices or similar units at educational institutions for students with disabilities

Literary Works:

- ○ Literary works distributed electronically (*i.e.*, e-books), for use with assistive technologies for persons who are blind, visually impaired, or have print disabilities
- ○ Literary works consisting of compilations of data generated by implanted medical devices and corresponding personal monitoring systems, to access personal data

Computer Programs and Video Games:

- ○ Computer programs that operate cellphones, tablets, mobile hotspots, or wearable devices (*e.g.*, smartwatches), to allow connection of a new or used device to an alternative wireless network ("unlocking")
- ◉ Computer programs that operate smartphones, tablets and other all-purpose mobile computing devices, smart TVs, or voice assistant devices to allow the device to interoperate with or to remove software applications ("jailbreaking")
- ○ Computer programs that control motorized land vehicles, including farm equipment, for purposes of diagnosis, repair, or modification of the vehicle, including to access diagnostic data
- ○ Computer programs that control smartphones, home appliances, or home systems, for diagnosis, maintenance, or repair of the device or system
- ○ Computer programs for purposes of good-faith security research
- ○ Computer programs other than video games, for the preservation of computer programs and computer program-dependent materials by libraries, archives, and museums
- ○ Video games for which outside server support has been discontinued, to allow individual play by gamers and preservation of games by libraries, archives, and museums (as well as necessary jailbreaking of console computer code for preservation uses only), and discontinued video games that never required server support, for preservation by libraries, archives, and museums
- ○ Computer programs that operate 3D printers, to allow use of alternative feedstock

Item C. Explanation of Need For Renewal

Provide a brief explanation summarizing the continuing need and justification for renewing the exemption. The Office anticipates that petitioners may provide a paragraph or two detailing this information, but there is no page limit. While it is permissible to attach supporting documentary evidence as exhibits to this petition, it is not necessary. Below is a hypothetical example of the kind of explanation that the Office would regard as sufficient to support renewal of the unlocking exemption. The Office notes, however, that explanations can take many forms and may differ significantly based on the individual making the declaration and the exemption at issue.

I am a Senior Staff Attorney at the Electronic Frontier Foundation, a nonprofit organization that advocates for the public in conversations about technology and digital policy. Part of EFF's mission is to protect the free expression and personal autonomy of technology users, as well as to advance innovation. In service of these values, EFF participates in regulatory procedures, lawmaking conversations, and impact litigation to support the rights of technology users to understand and control the software that runs their devices.

Exercising these freedoms continues to depend on 'jailbreaking' devices that include smartphones, tablets and other all-purpose mobile computing devices, smart TVs, or voice assistant devices. That is to say, TPMs exist on these devices that would adversely impact the ability of users to make noninfringing uses, such as accessing the computer programs that operate those devices to allow the device to interoperate with other technology or to remove software applications.

I have personal knowledge of the need to circumvent in reliance on the jailbreaking exemption as a result of my work. Some personal or publicly-documented examples include:

Personal Accounts: Smartphones

I recently locked myself out of an older smartphone for which I no longer remembered the password. Wanting to continue to use the hardware and firmware with a custom operating system, I performed a factory reset on the device, only to discover an anti-theft technology that required me to either input a password or to have previously entered a Google account on the device in order to continue to use the device. Not knowing the password and not having entered a Google account, the anti-theft technology would have rendered useless a phone worth several hundred dollars. Google support informed me that I could go in person (during the COVID pandemic) to a third-party authorized facility and attempt to persuade them that I had not stolen the device. If the device were over a year old, I would have to pay an unspecified fee even if I did persuade them. I was ultimately able to remember my password to this device, but many in this position will not be so fortunate and will continue to be affected by the TPM that prevents the noninfringing installation and use of software on Android phones (and removal of unwanted software) where authentication information has been lost.

I also broke the screen on another smartphone. While searching for ways to retrieve the data, I was fortunate to see that I had configured it in such a way that it would be interoperable with software on my laptop that could retrieve my data. I saw several solutions that would have circumvented access controls, and reports by individuals who had recently used these solutions to circumvent and regain access to their data by causing the phone to interoperate with software on their computers. I anticipate that people will continue to have a need to bypass TPMs in order to interoperate with software on covered devices that are not functioning or functioning in an unusual way, and to remove unwanted software interfering with that access.

Personal Accounts: Tablet and SmartTV

I purchased a used tablet from a stranger. Since I have no reason to trust the seller, I wanted to install fresh, secure software on the tablet, which required me to root the device before it would interoperate with the software I trusted and before I could remove existing software. I expect I and many others will continue to purchase used tablets and other covered electronics and wish to secure them, frequently depending on circumvention to do so as documented in the previous rulemaking and the resources below.

Item C. Explanation of Need For Renewal *(cont'd)*

In fact, the previous occupant of my home left a Smart TV and I have not enabled its wireless connections because I have not yet taken the time to jailbreak it and install trusted software. I would like the option to do this in the coming exemption period and, again, expect that others who obtain used devices – or even new devices – will want to ensure the software is trustworthy, particularly when SmartTVs can include cameras and microphones covering one's private living areas, as well as invasive tracking of one's browsing and viewing habits.

Third Party References

The iOS jailbreaking community continues to innovate, adding new features to old devices, such as the ability to use Apple's Siri software without needing to be plugged in to a power source. https://www.idownloadblog.com/2019/02/04/heysiri/ Tinkerers have also managed to get Android running on Apple hardware thanks to jailbreaking. https://9to5mac.com/2020/03/04/new-jailbreak-hack-lets-you-run-android-on-your-iphone-7/

The jailbreaks are also swiftly applied to new versions of the TPMs deployed for iOS, for a broad range of functionality such as picture-in-picture improvements, customization of pre-programmed events, additional power menu options, enhanced security options, power management, and more. https://piunikaweb.com/tag/jailbreak/; https://www.idownloadblog.com/tag/jailbreak/; https://www.idownloadblog.com/2020/05/25/10-reasons-to-jailbreak-ios-13/ This includes the Smartwatch version of iOS. E.g. https://piunikaweb.com/2019/12/27/change-notification-sounds-vibrations-watchos-jailbreak-tweak/ It also includes the Apple TV Smart TV version of iOS. E.g. https://www.idownloadblog.com/2019/11/13/checkra1n-tv-jailbreak-apple-tv/. Voice Assistant technology is also included, allowing interoperability with HomeKit home devices via a jailbroken smartphone emulating a Voice Assistant device such as a HomePod. https://limneos.net/homekithub/

In addition, software innovators continue to chafe at Apple's restrictive and expensive policies for the official App Store for iOS devices. http://www.iphonehacks.com/2020/06/phil-schiller-confirms-decision-hey-final.html Many users continue to jailbreak their devices in order to access alternative sources of apps and avoid Apple's walled garden, as discussed in prior rulemakings. See https://www.idownloadblog.com/jailbreak/#benefits (discussing alternative app sources Cydia, Installer, Sileo, and Zebra).

SmartTVs and voice assistant devices continue to overcollect private information without obtaining consent in a respectful manner. https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/; https://hackaday.com/2020/04/01/stay-smarter-than-your-smart-speaker/#more-404914. Some invasive features simply cannot be turned off within the default operating software. https://www.consumerreports.org/privacy/how-to-turn-off-smart-tv-snooping-features/ As per the previous rulemaking, users continue to have good reason to customize the software in their SmartTVs and Voice Assistants via jailbreaking to add and remove software applications, and will be adversely impacted in making these noninfringing uses absent a renewed exemption.

The need to jailbreak persists, and many of the same devices discussed in the previous rulemaking round are still in use today, and will be in the next three years. Absent a renewed exemption, users will be adversely affected in seeking to make the noninfringing uses protected by this exemption in the last rulemaking. I respectfully request that the Librarian renew this exemption.

Item D. Declaration and Signature

The declaration is a sworn statement made under penalty of perjury, and must be signed by one of the petitioners named above.

I declare under penalty of perjury under the laws of the United States of America that the following is true and correct:

1. **Based on my own personal knowledge and experience, I have a good faith belief that but for the above-selected exemption's continuation during the next triennial period (October 2021 – October 2024), technological measures controlling access to relevant copyrighted works are likely to diminish the ability of relevant users to make noninfringing uses of these works, and such users are likely to rely upon the above-selected exemption during the next triennial period.**

2. **To the best of my knowledge, there has not been any material change in the facts, law, or other circumstances set forth in the prior rulemaking record (available at https://www.copyright.gov/1201/2018) that originally demonstrated the need for the above-selected exemption, such that renewal of the exemption would not be justified.**

3. **To the best of my knowledge, the explanation provided in Item C above is true and correct, and supports the above statements.**

Name/Organization:

If the petitioner is an entity, this declaration must be signed by an individual at the organization having appropriate personal knowledge.

Kit Walsh
Electronic Frontier Foundation

Signature:

This declaration may be signed electronically (e.g., "/s/ John Smith").

/s/ Kit Walsh

Date:

July 22, 2020