Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109 USA
415.436.9333
eff.org

August 23, 2018

Regan Smith, regans@copyright.gov
Kevin Amer, kamer@copyright.gov
Anna Chauvet, achau@copyright.gov
VIA E-MAIL

RE: Docket No. 2017-10, Summary of Ex Parte Meeting with Copyright Office Staff Regarding Exemption to Prohibition Against Circumvention of Technological Measures Protecting Copyrighted Works – Class 7

Dear Ms. Smith,

Thank you for speaking with us by phone on August 21, 2018. Mitch Stoltz and the undersigned were on the call for the Electronic Frontier Foundation. Kevin Amer, Anna Chauvet, and Nicholas Bartelt were present for the Copyright Office. This letter summarizes our discussion of Class 7, EFF's proposed expansion of the exemption for accessing software and data compilations for purposes of noninfringing repair, diagnosis, and modification on devices not covered by the existing exemption for certain motor vehicle systems.

We reiterated that the need for circumvention to achieve these noninfringing uses is underscored by the introduction of Right to Repair legislation in many states, as well as the testimony of professionals who conduct the activities contemplated by the proposed class and the substantial interest garnered by online tutorials for such tinkering activities. We noted that the Office has acknowledged the barriers created in this context by the ban on circumvention in prior rulemakings and in its Section 1201 Report concerning tinkering activities. In particular, we noted that manufacturers have a clear economic incentive and history of using Section 1201 to attempt to achieve a monopoly on repair and follow-on innovation, a monopoly not intended by Congress and one that harms individuals, local business, and the environment.

We pointed out that the lawful ability to add and remove software from one's own multipurpose device cannot turn on whether or to what extent that device is used to access entertainment content, because such a criterion would imperil a wide range of lawful activities.

We noted that opponents did not include any evidence that the ability to repair or modify devices presents a particularized risk of enabling copyright infringement. Rather,

they theorized about convoluted ways that a determined person *could* extract copyrighted music from an abstract, unspecified device, but did not present evidence that this was likely to occur in any significant amount if the exemption is granted. We pointed out that other opponents have raised the same argument, with a similarly weak evidentiary basis, with respect to smartphones in three previous rulemaking cycles, and the Register has nonetheless granted exemptions for jailbreaking (and thus modification) continuously since 2010. Anecdotal evidence and conjecture aside, the past eight years have demonstrated that the ability to modify multipurpose computing devices does not significantly increase infringement, nor does it measurably decrease revenues for music, video, books, games, or software. The theoretical possibility of infringement is even more remote for repair and diagnosis alone.

You asked about the types of TPMs that are used in connection with streaming media on devices that provide such functionality. We explained that devices often employ multiple TPMs, including account verification and activity pattern analysis on the server side, which are neither covered by the proposed exemption nor accessible to device owners. We further explained that streaming media such as music often employs TPMs that are distinct from the TPMs that control access to the device firmware (and thus are not covered by this proposed exemption). However, even in instances where the access controls on device firmware also confer additional control over access to entertainment content, the lawful ability to jailbreak should be preserved. Otherwise, rightsholders who supply device firmware (or control its design through contractual agreements and patent licenses with manufacturers) will effectively be able to take away device owners' ability to modify their own devices based on the specifics of firmware design.

You also asked whether streaming media content is ever available in unencrypted form on a device. We explained that digital media is always decrypted at some point in the playback process and can theoretically be accessed at that point, but that such access is often extremely difficult and impractical and that opponents have not identified a means of achieving this access that they believe would avoid Section 1201 liability.

EFF appreciates the time and thoughtful consideration of the Copyright Office staff on these issues.

Respectfully submitted,

Kit Walsh
Senior Staff Attorney
Electronic Frontier Foundation