UNITED STATES COPYRIGHT OFFICE

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

Reply Comments of the Electronic Frontier Foundation on Proposed Class 6 – Jailbreaking

ITEM A. COMMENTER INFORMATION

Electronic Frontier Foundation
Mitchell L. Stoltz
815 Eddy St
San Francisco, CA 94109
(415) 436-9333
mitch@eff.org

The Electronic Frontier Foundation (EFF) is a member-supported, nonprofit public interest organization devoted to maintaining the traditional balance that copyright law strikes between the interests of rightsholders and the interests of the public. Founded in 1990, EFF represents over 44,000 dues-paying members, including consumers, hobbyists, artists, writers, computer programmers, entrepreneurs, students, teachers, and researchers, who are united in their reliance on a balanced copyright system that ensures adequate incentives for creative work while promoting innovation, discouraging censorship, and enabling broad and equal access to information in the digital age.

ITEM B. PROPOSED CLASS ADDRESSED

We submit these reply comments in support of Proposed Class 6 - Jailbreaking.

ITEM C. OVERVIEW

Voice assistant or "smart speaker" devices continue to grow in importance as a new class of consumer device, designed to carry out a wide variety of computing tasks. In their versatility, and in the basics of their design and operation, these devices resemble mobile computing devices like smartphones and tablets. And like mobile computing devices, the versatility and power of voice assistant devices creates a demand for customization beyond the limits set by manufacturers—including a demand for finer control over these devices' handling of personal information. What makes voice assistants distinct is that voice interaction is central and indispensable to their use.

Thanks to exemptions granted by the Librarian, circumvention of access controls in order to install new software on a smartphone—a process known colloquially as jailbreaking or rooting—has been permitted under 17 U.S.C. § 1201(a)(1) for eight years. And in *three* rulemaking cycles, from 2012 through 2017, no smartphone manufacturer has opposed that exemption. The reason why is clear: far from harming the market for mobile computing devices and applications, the ability to jailbreak has complemented and enhanced these markets, spurring new thinking in application development and driving demand for new hardware. Moreover, mobile devices like phones and tablets are now

one of the main channels through which U.S. consumers buy copyrighted media.[1] The growth of these markets for creative work has happened simultaneously with the lawful ability to jailbreak the devices that have driven that growth.

All of the same factors are in place today for voice assistants. There is another similarity as well: no manufacturer of voice assistant devices objects to their inclusion in an expanded jailbreaking exemption.

Two opposition comments raise generalized arguments about the use of access controls to prevent infringement and to restrict the functionality of lawfully purchased computing devices. But these comments fail to explain how the ability to jailbreak voice assistants in particular raises a greater threat of infringement than the ability to jailbreak the vast universe of other general-purpose computing devices for which it has long been permitted. Eight years of real-world experience with jailbreaking of other general-purpose consumer devices on a grand scale make it clear that opponents' speculations about the use of smart speakers for infringing purposes are just that: unsubstantiated speculation.

The Motion Picture Association of America et al. also attempt to raise new procedural hurdles in this rulemaking by suggesting that exemption proponents cannot propose a narrower, more focused definition of a class of works in their comments—even when such a proposal responds directly to the Register's own request for clarification. MPAA's suggestion is at odds with the entire history of this rulemaking process, and finds no support in the statute. The Office should reject it, and grant EFF's petition.

ITEM D. TECHNOLOGICAL PROTECTION MEASURE(S) AND METHOD(S) OF CIRCUMVENTION

1. Voice Assistant Devices Are A Well-Defined Class of Devices and Are Similar to Smartphones and Tablets in All Relevant Ways.

EFF's September 13, 2017 petition proposed an expansion of the existing jailbreaking exemption to cover certain similarly situated devices. The paradigmatic examples of this expansion class were listed: "the Amazon Echo series of products, the Google Home, and the forthcoming Apple HomePod."[2] The Register requested public comment on this class in the Notice of Proposed Rulemaking. The Register specifically requested comment on definitions of terms to be used in an expanded exemption class, and on "examples of specific types of devices that would be encompassed by the exemption other than those enumerated in the existing exemption."[3]

---

[1] For example, a market research group found that "60% of streaming activity is done via mobile devices." Kate Kaye, "GroupM: Mobile Music Streaming Represents $220M Ad Opportunity," AdAge (Dec. 29, 2016), http://adage.com/article/datadriven-marketing/groupm-sees-mobile-music-streaming-untapped-ad-spend/307321/.

[2] Electronic Frontier Foundation, Petition for a New Exemption at 3, *available at* https://www.copyright.gov/1201/2018/petitions-091317/class6/class-06-newpetition-eff.pdf (EFF Petition).

[3] *Exemptions to Permit Circumvention of Access Controls on Copyrighted Works: Notice of Proposed Rulemaking*, 82 Fed. Reg. 49550, 49560-61 (Oct. 26, 2017) ("NPRM").

On December 18, 2017, EFF, the Owners' Rights Initiative, and the Association of Service and Computer Dealers International filed opening comments presenting evidence that Section 1201's ban on circumvention adversely impacts non-infringing uses of voice assistant devices in the same way as smartphones and other devices covered by the existing exemption. Responding to the NPRM, EFF et al. also proposed more focused regulatory language and a new definition to make clear what devices an expanded exemption will cover, with proposed additions in bold:

> *Computer programs that enable smartphones,* ***voice assistant devices,*** *and portable all-purpose mobile computing devices to execute lawfully obtained software applications, where circumvention is accomplished* ***solely for one or more of the following purposes:*** *enabling interoperability of such applications with computer programs on the smartphone or device, or to permit removal of software from the smartphone or device,* ***or to enable or disable hardware features of the smartphone or device.*** *For purposes of this exemption, a "portable all-purpose mobile computing device" is a device that is primarily designed to run a wide variety of programs rather than for consumption of a particular type of media content, is equipped with an operating system primarily designed for mobile use, and is intended to be carried or worn by an individual.* ***A "voice assistant device" is a device that is primarily designed to run a wide variety of programs rather than for consumption of a particular type of media content, is designed to take user input primarily by voice, and is designed to be installed in a home or office.***[4]

This revision makes clear that the proposed class excludes television set-top boxes and video game consoles.[5] In addition, to better capture the class of devices described, EFF et al. proposed to limit the expanded exemption class to devices that are "designed to take user input *primarily* by voice."[6] This limitation is unambiguous. The Amazon Echo family of devices, the Google Home products, the Apple HomePod, and similar devices such as the Microsoft Invoke and the Sonos One, are designed almost entirely around voice input. While they typically have several buttons to control volume, microphone mute, and track skipping, they are not designed to be operated by touch alone.[7] Moreover, advertising for these devices highlights the primacy of voice input.[8]

---

[4] Comment of EFF, ORI, and ASCDI on Proposed Class 6, at 2.

[5] *See* Opposition Comment of Entertainment Software Association at 2 ("ESA") (acknowledging that EFF et al.'s opening comments proposed "narrower regulatory language" which "distinguished voice assistant devices from other kinds of devices, including desktop and laptop computers and video game consoles.").

[6] Initial Comment of EFF, ORI, and ASCDI at 2 ("Initial Comment") (emphasis added).

[7] The HomePod's touch surfaces can be used for "volume up/down," "play/pause music," waking the voice assistant, and skipping tracks. HomePod, https://www.apple.com/homepod/specs/ (visited March 14, 2018).

[8] *See, e,g,* Google Home Max, https://store.google.com/product/google_home_max_smart_home (visited March 14, 2018).

The opposition comments of MPAA et al., and those of ACT, recognize that EFF's proposal relates to voice assistant devices.[9] However, they misstate the breadth of EFF's proposal. EFF's proposed revision to the jailbreaking exemption does not encompass all devices "capable of being operated by voice,"[10] nor "all software-enabled consumer products with voice assistant functionality."[11] While MPAA mentions various devices that accept voice commands, these examples are excluded from EFF's proposed definition on two separate grounds. First, the set-top boxes, digital video recorders, and universal remote controls cited by MPAA are all fully functional *without* using voice commands, as all of them accept universal input through pressing buttons.[12] Second, none of MPAA's examples are designed to run a wide variety of software applications apart from media viewing. These two factors distinguish the devices listed in EFF's petition, and in its initial comments, as a particular class of devices. They also exclude game consoles and set-top boxes.

MPAA's claim that "voice assistants . . . are outside the scope of the proposed class of works at issue"[13] is simply bizarre, given that EFF's petition specifically named the Amazon Echo, Google Home, and Apple HomePod as paradigmatic examples of the proposed class.[14] MPAA et al. cannot claim in good faith to be prejudiced by EFF's suggestion on how to refine and clarify the regulatory definition of these devices, particularly since those clarifications respond directly to the Register's questions in the NPRM. Indeed, ESA, which joined MPAA's comment, acknowledged in a separate comment that EFF's second proposal was a narrowing of its initial petition.[15] ESA, writing separately, expressed no opposition to a jailbreaking exemption for voice assistants that excludes video game consoles.[16]

When an exemption proponent has shown an adverse effect on non-infringing uses of works, the Register is required to grant an exemption.[17] Proponents of expanding the jailbreaking exemption to include voice assistants have made such a showing. The Register has indicated that the Copyright Office will continue to draft final regulatory language for each exemption class for

---

[9] Opposition Comment of the Motion Picture Association of America, Recording Industry Association of America, Entertainment Software Association, and Association of American Publishers at 4 ("MPAA"); Opposition Comment of ACT | The App Association at 2 ("ACT").
[10] MPAA at 10.
[11] ACT at 6.
[12] *See* Xfinity.com, "The X1 Voice Remote Overview," https://www.xfinity.com/support/articles/get-to-know-xr11-remote (accessed March 14, 2018) (showing remote buttons, including arrow keys for visual navigation); Janko Roettgers, "TiVo Releases New Devices with Voice Control, May Add Alexa Support Next," Variety (Oct. 24, 2017), http://variety.com/2017/digital/news/tivo-bolt-vox-voice-control-alexa-1202597408/ (similar); Best Buy, "Logitech – Harmony Elite Universal Remote – Black," https://www.bestbuy.com/site/logitech-harmony-elite-universal-remote-black/4314901.p (accessed March 14, 2017) (similar).
[13] MPAA at 9.
[14] EFF Petition at 3.
[15] ESA at 2.
[16] *Id.*
[17] 12 U.S.C. § 1201(a)(1)(B)("The prohibition contained in subparagraph (A) *shall not apply*. . . ") (emphasis added).

recommendation to the Librarian based on the evidence and arguments presented.[18] MPAA's argument that proponents have a "burden of proffering a definition" in their initial petitions which cannot be narrowed in the course of proceedings is contrary to the statute,[19] the *Section 1201 Report*,[20] and MPAA's own assertions in previous rulemakings.[21] It must be rejected.

2. The Proposed Class Covers General-Purpose Devices and Will Not Harm to Entertainment Content or Encourage "Counterfeit Apps"

Opposition to a proposed class must be based on substantive evidence, not speculation about potential harms.[22] The comments of MPAA et al. and ACT concerning potential infringement of "subscription entertainment" and "counterfeit apps" do not meet that standard. In particular, they fail to explain why infringement is more likely on voice assistant platforms than on smartphones, tablets, and other devices already subject to an exemption—or on personal computers, where such works are equally available.

The Register has recognized that the exemption for jailbreaking smartphones has not contributed to the infringement of entertainment content in any significant way.[23] Moreover, rightsholders for music, video, ebooks, and games continue to make their works available by the millions on smartphones and tablets. All of the subscription content platforms listed in MPAA's comments, including "Spotify, Amazon Music Unlimited, YouTube Red, Apple Music, Pandora, and SiriusXM"[24] are available through apps on mobile devices that have long been subject to an exemption. Yet MPAA et al. point to no evidence that unauthorized access to subscription content is more prevalent on mobile devices because of the legal ability to jailbreak. Likewise, subscription content is widely available through apps or browser plugins on personal computers running Windows and MacOS. Personal computers give root or superuser privileges to their owner or primary user by default.[25] The relative openness of those platforms has not caused rightsholders to withhold their content.

---

[18] 1201 Report at 150 (declining to solicit comment on recommended regulatory language).
[19] 17 U.S.C. § 1201(a)(1)(D) (requiring the Librarian to designate exemption classes).
[20] *Section 1201 of Title 17: A Report of the Register of Copyrights* (June 2017) at 110 ("Section 1201 Report") (noting that the statute does not assign any "burden of production").
[21] *See, e.g., Section 1201 Rulemaking: Sixth Triennial Proceeding, Recommendation of the Register of Copyrights* at 101 ("2015 Recommendation") ("Joint Creators have suggested that the phrase 'noncommercial videos' should be narrowed to help distinguish this category from the educational use exemptions.").
[22] NPRM at 49558 "[C]ommenters (both proponents and opponents) should be aware that the Office favors specific, 'real-world' examples supported by evidence over speculative, hypothetical observations.").
[23] In 2012, MPAA et al. argued that the ability to jailbreak smartphones would "harm[] the overall copyright ecosystem that tethered devices enable copyright owners to exploit." Section 1201 Rulemaking: Fifth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Report of the Register of Copyrights at 70 (Oct. 2012). Rejecting this assertion, the Register determined that the record showed "at best, only a tenuous relationship between jailbreaking of smartphones and piracy." *Id.* at 76-77.
[24] MPAA at 11.
[25] Exhibit 1, Statement of Seth Schoen ¶ 4.

One reason for this is that rightsholders employ access controls that function even if the device owner has root privileges. As EFF Senior Staff Technologist Seth Schoen explains in the attached statement, root privileges are typically not sufficient to give the owner unrestricted access to entertainment media, because application software used to decrypt and view those media enforces other restrictions or contains other technical measures that do not depend on withholding root privileges.[26]

In addition, rightsholders for entertainment content use server-side access controls that are also unaffected by customers' control over the devices they own. For example, a service provider can restrict the number of simultaneous streams each customer can run.[27] It can also analyze connections to its servers for unusual patterns of activity, such as connections from multiple Internet Protocol addresses presenting the same credentials, when those addresses appear to be assigned to devices that are geographically far away from one another.[28] A server can easily be configured to prevent "large numbers of recordings being obtained faster than they could be listened to in real time,"[29] simply by limiting the rate of downloading when certain criteria are met.[30]

Both application-layer access controls and server-side access controls are applied to subscription entertainment content on a variety of devices. MPAA does not explain why securing entertainment content on voice assistant devices requires that owners be prevented from adding or removing software, when the same does not hold true for smartphones, tablets, and personal computers. And MPAA presents no evidence of any fundamental difference between voice assistants and other personal computing devices that would make infringement more likely on voice assistants if an exemption is granted.

For the same reasons, MPAA's suggestion that an exemption should be limited to installing "apps that lawfully access content" is not warranted. Smartphones, tablets, and PCs are not subject to any such restriction, yet the ability to jailbreak has not contributed significantly to infringement. Such a restriction would be unworkable in practice, as it would cause the legality of jailbreaking to depend on which apps were subsequently installed. Moreover, an exemption so limited would fail to alleviate the adverse impact of the access controls on non-infringing uses. Any number of lawful and valuable applications nonetheless have the potential to "enable unauthorized access to copyrighted works," including general-purpose applications like Web browsers.

ACT's discussion of "counterfeit apps" suffers from the same lack of particularity. The Register has never found that the mere *ability* to load counterfeit software on a general-purpose computing device justifies denying owners the right to install software of their choice. As ACT provides no examples of counterfeit software for a voice assistant device, nor any reason why such software presents a greater problem on voice assistant devices than on smartphones, there is no basis for the Register to change course on this issue. It should go without saying that ACT's general policy

[26] *Id.* ¶ 5-6.
[27] *Id.* ¶ 7.
[28] *Id.* ¶ 7.
[29] MPAA at 12.
[30] Statement of Seth Schoen ¶ 7.

preferences about the "app ecosystem" or their views on the importance of "copyright protection" have no bearing on this proposal to expand the jailbreaking exemption.[31] As the Register has determined, comments that "largely re-articulate[] a general opposition to a jailbreaking exemption" are not meaningful.[32] In the renewal phase of these proceedings, the Register rejected[33] a similar unsupported assertion by BSA that jailbreaking "facilitates copyright infringement."[34]

3. No Reasonable Alternative to Circumvention Exists.

As described in EFF's initial comments, the non-infringing use being impacted is the ability to alter the functionality of devices that one already owns. Voice assistant devices are powerful and sophisticated computers whose capability for non-infringing use should be limited only by the imaginations of their owners, not the preferences of their manufacturers. In particular, users of these devices need the ability to selectively *limit* their functionality, such as by limiting the reach of the always-on voice recognition, the various wireless interfaces, and the transmission of very personal data. These and other important modifications require adding software to the device itself, and cannot be accomplished through "Alexa Skills" and similar third-party functionality that resides largely on the manufacturer's servers.

MPAA's dismissal of these concerns as "mere inconvenience" is contrary to the Register's historic approach to similar issues. Indeed, the Register rejected this very argument with respect to mobile devices.[35] The Apple HomePod, currently on sale, contains access controls that do not allow the installation of any third-party apps. Jailbreaking is thus the *only* way to add non-Apple software to a HomePod. MPAA's speculation[36] about whether Apple might change its policy in the future does not obviate the need for an exemption now. And because the HomePod runs a version of iOS, the same operating system used on Apple's iPhone and iPad devices, developers in the jailbreaking community will be able to leverage work already done on that platform to create new, useful voice applications.

Finally, the "open source electronics platforms" cited by ACT are not substitutes for voice assistant devices. Raspberry Pi and Arduino are circuit boards that can be used as a component in electronics projects.[37] Building a device from scratch to approximate the functionality of a voice assistant such as the Echo requires more than a development board such as a Raspberry Pi or an Arduino—it requires input and output devices, a network interface, buttons and indicator lights, power supply

---

[31] ACT at 3-5.
[32] NPRM at 14-15.
[33] *Id.* at 15;
[34] Comment of BSA | The Software Alliance at 1 (Sep. 13, 2017).
[35] 2015 Recommendation at 190 (rejecting the argument that purchasing a new device is a sufficient alternative to jailbreaking).
[36] MPAA at 14.
[37] *See* "Adafruit's Raspberry Pi Lesson 4. GPIO Setup" (Dec. 14, 2012), https://learn.adafruit.com/adafruits-raspberry-pi-lesson-4-gpio-setup (describing methods of attaching input and output devices to a Raspberry Pi board); "Ladyada's Learn Arduino – Lesson 0" (Jul. 14, 2016), https://learn.adafruit.com/ladyadas-learn-arduino-lesson-number-0 (describing Arduino as "an open source prototyping platform" that "has been the brain of thousands of projects.").

circuitry, a durable physical housing, and significant assembly and programming.[38] The cost of such a project is likely to be more than the retail price of a mass-produced voice assistant device.[39] In short, development boards are no more a substitute for a voice assistant device than an engine is a substitute for an automobile.

In summary, EFF has defined a class of works—firmware on voice assistant devices—and shown how access controls on these works adversely impact important, valuable non-infringing uses of those devices. The comments in opposition express a general preference for access controls that restrict what consumers can do with their own devices, but present no countervailing evidence that is specific to this class of works. Accordingly, we ask the Register to recommend expanding the existing, highly successful exemption for jailbreaking to include the closely related category of voice assistant devices.

ITEM F. DOCUMENTARY EVIDENCE

Eff submits Attachment 1, the Statement of Seth Schoen, as documentary evidence.

[38] For example, a kit for building a basic voice-activated device using a Raspberry Pi costs $149.95. It requires soldering of components and compilation of software code, along with other assembly steps. Maryam Ashoori, "Control an LED With Your Voice Using Watson and Raspberry Pi," https://learn.adafruit.com/tjbot-control-an-led-with-your-voice-watson-on-raspberry-pi?view=all (accessed March 14, 2017).
[39] *Id.*

Attachment 1 to Reply Comments of the Electronic Frontier Foundation on Proposed Class 6 – Jailbreaking

Statement of Seth Schoen
Regarding Proposed Class 6 - Jailbreaking

1. My name is Seth Schoen. I am a Senior Staff Technologist at the Electronic Frontier Foundation (EFF). I have worked with computers and computer networks for twenty years. I have published two peer-reviewed academic papers in the field of computer security, and been interviewed about computer networking and computer security in the national news media. I have testified about electronic communications systems in three courts and before the Copyright Office and the United States Sentencing Commission.

2. I have experience with technological protection measures from assisting attorneys in litigation related to these measures, as well as with prior iterations of the present rulemaking process. I also attended meetings of industry organizations related to TPMs, such as the Copy Protection Technical Working Group and the Digital Video Broadcasting forum, for several years.

3. In this statement, I respond to assertions made by Christopher Bell, VP Technology and Anti-Piracy, Warner Music Group, in his written statement related to jailbreaking of voice assistant or smart speaker devices.

4. Voice assistants are among the many types of devices that can be used to access streaming services, along with smartphones, tablets, personal computers, and other devices. These devices vary widely in their openness to user control and modification. Personal computers are generally configured to give their owner or primary user "root" or "superuser" privileges or the equivalent. This means the user can, with limited exceptions, add, remove, and replace software at will, and often thereby enable or disable the device's functions. Smartphones and tablets generally do not give the owner or primary user these privileges by default, but they can be "jailbroken" or "rooted" in order to do so.

5. On each of these types of devices, a streaming service that wishes to authenticate a user can use one or more measures to do so, including hardware identifiers, network identifiers, stored keys or tokens, user logins and passwords, and measures that reside on the streaming server or elsewhere on the Internet. While some of these measures require that the device owner or user does not have root privileges on their device, many will function even if the device owner has such privileges.

6. For example, owners of personal computers running Windows or macOS typically have root or "administrator" privileges and can add or remove any software they choose. Yet industry has arranged for these devices to access media that is restricted by encryption and other technical measures, including video from DVD and Blu-Ray discs, streaming video, digital radio, ebook subscription, and digital music download services. The device owner's root privileges typically are not sufficient to give the owner unrestricted access to those media, because the application software used to decrypt and view those media enforces

other restrictions or contains other technical measures that do not depend on controls in the operating system. In some cases, TPMs do have an operating system component, but the exercise of root privileges does not directly or automatically disable such a component.

7. Streaming media services can also use a variety of measures on the server side to enforce policies about authorized access to media. These measures do not depend on locking the user's device against modification. For example, a service provider can restrict the number of simultaneous streams each customer can run. It can also analyze connections to its servers for unusual patterns of activity, such as connections from multiple Internet Protocol addresses presenting the same credentials, when those addresses appear to be assigned to devices that are geographically far away from one another. In particular, a server can easily be configured to prevent "large numbers of recordings being obtained faster than they could be listened to in real time," by limiting the rate of downloading when certain criteria are met.

8. Because streaming services are provided on a variety of devices that vary in their level of openness to owner modification, I believe that service providers use a variety of authentication measures and access controls that do not depend on withholding root privileges from the device owner.

Seth Schoen
March 14, 2018