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

Please submit a separate comment for each proposed class.

NOTE: This form must be used in all three rounds of comments by all commenters not submitting short-form comments directly through regulations.gov, whether the commenter is supporting, opposing, or merely providing pertinent information about a proposed exemption.

When commenting on a proposed expansion to an existing exemption, you should focus your comments only on those issues relevant to the proposed expansion.

[ ] Check here if multimedia evidence is being provided in connection with this comment

Commenters can provide relevant multimedia evidence to support their arguments. Please note that such evidence must be separately submitted in conformity with the Office's instructions for submitting multimedia evidence, available on the Copyright Office website at https://www.copyright.gov/1201/2021.

ITEM A. COMMENTER INFORMATION

Identify the commenter and provide a means to contact the commenter and/or the commenter's representatives, if any.

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 35,000 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.

Inquiries concerning this comment can be directed to:

Mitch Stoltz
Senior Staff Attorney
mitch@eff.org
415-436-9333

Kit Walsh
Senior Staff Attorney
kit@eff.org
415-436-9333

ITEM B. PROPOSED CLASS ADDRESSED

Identify the proposed exemption that the comment addresses by the number and name of the class set forth in the Notice of Proposed Rulemaking (e.g., "Proposed Class 1: Audiovisual Works—Criticism and Comment").

We submit these comments in support of Proposed Class 11: Computer Programs—Jailbreaking. In 2015, the Register recommended, and the Librarian granted, an exception for

> *[c]omputer programs that enable smart televisions to execute lawfully obtained software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications with computer programs on the smart television.*

This exemption was renewed without objection in 2018. The Software Freedom Conservancy has petitioned for its renewal in the current exemption cycle, and it received no objections.

EFF petitions the Librarian to clarify that a "smart television" in this exemption need not have an integrated display screen, to make it clear that the exempted class includes computer programs on ***devices that are primarily designed to display software applications on a screen, including applications that stream video delivered via the Internet, where such devices connect to but are not physically integrated into a display***. Alternatively, we ask the Librarian to grant an exemption for such devices that is equivalent to the existing exemption for smart TVs. Paradigmatic examples of the devices for which we seek an exemption are the Amazon Fire TV,[1] the Apple TV,[2] and the Roku.[3] Another term for these devices is "over-the-top" (OTT) set-top boxes, which refers to devices that stream video from the Internet rather than from an FCC-regulated multichannel pay-TV service such as cable.

ITEM C. OVERVIEW

Provide a brief summary of the circumvention activity sought to be exempted or opposed and why.

"Jailbreaking" is a colloquial term for practices that allow owners of computing devices to install or remove software of their choosing. On some operating systems, this is referred to as "rooting"; this comment uses the term jailbreaking regardless of the operating system involved. Jailbreaking requires circumventing access controls imposed by the manufacturer that would otherwise prevent the installation or removal of software. The Register of Copyrights has recommended, and the Librarian of Congress has enacted exemptions relating to jailbreaking in four previous triennial rulemaking cycles, beginning in 2010. To date, these exemptions have included smartphones,

[1] "All-new Fire TV Stick with Alexa Voice Remote 2020 release," Amazon.com, https://www.amazon.com/dp/B07ZZVX1F2 (accessed Dec. 13, 2020).

[2] "AppleTV," https://www.apple.com/tv/ (accessed Dec. 13, 2020).

[3] "Roku," https://www.roku.com/ (accessed Dec. 13, 2020).

tablets, wearable and other mobile computing devices, voice assistant or "smart speaker" devices, and smart TVs.

Most if not all of the devices in these categories include access controls that limit the owner's ability to install new software on the device, or to remove software. Jailbreaking means modifying the firmware or operating system on the device to circumvent or disable those access controls.

Video streaming devices are functionally and architecturally identical to smart TVs, except that they are physically separate from the display itself, typically connecting to it through an input port.[4] In either case, they are computing devices that run a variety of programs, including but not limited to programs that play video streams received over the Internet.

Device owners jailbreak their video streaming devices for the same reason that one would jailbreak a fully integrated smart TV with a display: to exercise full control over a powerful and valuable computing device and make it suit their needs. This includes adding functionality, such as the ability to view incoming phone calls or messages and browse the web; enabling compatibility with other hardware, including game controllers; and sending video streams to and from other devices. It also includes enhancing one's privacy and security by running virtual private network (VPN) software or disabling user tracking. And it includes changing the device's user interface to suit the owner's needs and preferences, such as by replacing the home screen. Jailbreaking makes these uses possible in circumstances that the device manufacturer did not foresee or approve in advance.

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

Describe the technological protection measure(s) that control access to the work and the relevant method(s) of circumvention. It would be most helpful to the Office if sufficient information is provided to allow the Office to understand the nature and basic operation of the relevant technologies, as well as how they are disabled or bypassed.

The technological protection measures used on video streaming devices are very similar to the measures used on mobile computing devices, because video streaming devices use derivatives of the same firmware and operating systems that are used by mobile computing devices. In particular, many of these devices run derivatives of Apple's iOS and Google's Android operating systems.

a. tvOS on the Apple TV: Cryptographic Verification of All Software

The AppleTV devices run "tvOS," a derivative of the iOS operating system that Apple uses on its mobile devices.[5] Like iOS devices, AppleTV devices are subject to severe restrictions on the

[4] For example, "Roku TVs" are smart TVs made by numerous manufacturers that incorporate Roku hardware and software, providing apps, a voice assistant, and integration with some Apple devices. "Roku TV," https://www.roku.com/products/roku-tv (accessed Dec. 13, 2020). Roku "streaming players," such as the Roku Premiere, run the same software and incorporate the same functionality but in a physically separate enclosure that connects to a display through an HDMI cable. "Roku Premiere," https://www.roku.com/products/roku-premiere (accessed Dec. 13, 2020).

[5] TvOS is "an operating system for Apple TV that was built from iOS." Lory Gil, "Apple TV update: Everything you need to know about tvOS 14," iMore (Sep. 22, 2020),

loading, running, and deletion of software. They employ cryptographic verification that prevents any application from running on a device unless it bears a digital signature from Apple.[6] They also contain cryptographic checks at various levels of the software stack that prevent modification or replacement of the operating system itself.[7] The current models of the AppleTV—the 4K and HD models—are able to download and install some apps from Apple's App Store,[8] but many apps that will run on other Apple devices are blocked from installation on an AppleTV. Older models of AppleTV cannot access the App Store. Under normal conditions, owners of these older devices cannot choose the software that is installed on their devices at all:

> When the Apple TV debuted, it had less than a dozen channels of Internet content. By the time Apple stopped making these models, there were dozens. . . . There was generally no warning when new channels appeared, and users couldn't control if they were installed or not. When you turned your Apple TV on, you'd find that a new icon had appeared on the home screen and that you now had new content available."[9]

---

https://www.imore.com/tvos-14. Apple describes the developer environment for tvOS as employing "many of the same frameworks, technologies, and concepts that are similar to iOS." "TvOS," Apple Developer Portal, https://developer.apple.com/tvos/ (accessed Dec. 13, 2020).

[6] Apple Inc., "Hardware Security Overview," https://support.apple.com/en-ca/guide/security/secf020d1074/1/web/1 (accessed Dec. 13, 2020) ("Apple devices—running iOS, iPadOS, macOS, watchOS, or tvOS—have security capabilities designed into silicon."); Apple Inc., "Apple Platform Security: Mandatory code signing," https://support.apple.com/en-ca/guide/security/sec7c917bf14/web (accessed Dec. 13, 2020) ("To ensure that all apps come from a known and approved source and haven't been tampered with, iOS and iPadOS require that all executable code be signed using an Apple-issued certificate."); Apple Inc., "Apple Platform Security: iOS and iPadOS app security overview," https://support.apple.com/en-ca/guide/security/secf49cad4db/web (accessed Dec. 13, 2020) ("iOS and iPadOS don't allow users to install potentially malicious unsigned apps from websites, or run untrusted apps. At runtime, code signature checks of all executable memory pages are made as they are loaded to ensure that an app hasn't been modified since it was installed or last updated.").

[7] Apple Inc., "Apple Platform Security: iOS and iPadOS secure boot chain," https://support.apple.com/en-ca/guide/security/secb3000f149/web (accessed Dec. 13, 2020) ("Each step of the startup process contains components that are cryptographically signed by Apple to ensure integrity and that proceed only after verifying the chain of trust. This includes the bootloaders, the kernel, kernel extensions, and baseband firmware. This secure boot chain helps ensure that the lowest levels of software aren't tampered with.").

[8] Sam Costello, "Can You Install Apps on the Apple TV? Stream TV, movies and music on your Apple TV by installing apps," Lifewire (Sep. 11,2020), https://www.lifewire.com/can-you-install-apps-on-the-apple-tv-1999690.

[9] *Id.*

b. Amazon Fire OS and Roku Firmware: Lack of Access to Root Privileges

Amazon's streaming devices run "Fire OS," a derivative of Google's Android operating system, which is itself a derivative of the GNU/Linux operating system used on millions of devices worldwide. GNU/Linux contains access controls that can be configured to restrict access to nearly any of a device's functions, including the ability to add or remove software from a device.[10] When those access controls are enabled, modifying the functioning of the device requires root, or superuser, access to the device.[11]

Amazon's devices don't give root access to the owner of the device.[12] While it is possible to install some applications onto a Fire TV device from unapproved sources (known as "sideloading,") there are limits to what these applications can do. In particular, they cannot modify the overall user experience of the device.[13]

Roku devices use proprietary firmware. They contain a "channel store" that permits loading applications from a relatively small catalog selected by Roku. The devices don't allow sideloading of apps from other sources, or replacement of the firmware.[14]

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

Comments should be directed at answering the following question: Are users of a copyrighted work adversely affected by the prohibition on circumvention in their ability to make noninfringing uses of a class of copyrighted works, or likely to be so adversely affected in the next three years? Commenters are encouraged to focus on the following elements:

- *Whether the proposed class includes at least some works protected by copyright.*
- *Whether the uses at issue are noninfringing under title 17.*
- *Whether users are adversely affected in their ability to make such noninfringing uses or, alternatively, whether users are likely to be adversely affected in their ability to make such noninfringing uses during the next three years. Discussion of this element should include an evaluation of section 1201(a)(1)(C)'s five statutory factors: (i) the availability for use of copyrighted works; (ii) the availability for use of works for nonprofit archival, preservation, and educational purposes; (iii) the impact that the prohibition on the*

[10] James Morris, "Overview of Linux Kernel Security Features," The Linux Foundation (July 11, 2013), https://www.linux.com/learn/overview-linux-kernel-security-features.

[11] *Id.* ("Running a program as the superuser provides that program with all rights on the system.").

[12] *See, e.g.* Elias Saba, "How to Root the Amazon Fire TV," AFTVnews (June 15, 2014), https://www.aftvnews.com/how-to-root-the-amazon-fire-tv/ (describing the steps required to enable root access on a Fire TV device).

[13] Exhibit A, Statement of David Drager.

[14] Ivacy, "How to Jailbreak Roku in 2020," https://www.ivacy.com/blog/how-to-jailbreak-roku-tv/ (May 10, 2020) (explaining that viewing third-party app content through a Roku requires additional hardware).

circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research; (iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and (v) such other factors as the Librarian considers appropriate.

- *Whether the statutory prohibition on circumventing access controls is the cause of the adverse effects.*

This section should identify all statutory provisions, case law, and/or other legal authority the commenter wishes the Office to consider in connection with the proposed class. Commenters should also provide an evidentiary basis to support their arguments, including discussion or refutation of specific examples of adverse effects on noninfringing uses and, if available, relevant documentary and/or multimedia evidence.

Commenters should demonstrate, or refute, that the asserted adverse effects are real, tangible, and concrete, and not merely hypothetical, theoretical, or speculative—that is, they are not merely possible, but probable. This discussion should include an evaluation of section 1201(a)(1)(C)'s five statutory factors. For example, in analyzing the first statutory factor, commenters should examine whether there are any potential alternatives that permit the asserted noninfringing use(s) without the need for circumvention, and whether such potential alternatives are realistic options.

1. Jailbreaking Video Streaming Devices Is Non-Infringing

The works at issue in this request are firmware and operating system programs installed on video streaming devices, which are subject to copyright. Jailbreaking involves modifying those programs, potentially creating a derivative work. Nonetheless, it does not infringe copyright, because it is a fair use.[15] Fair use is "a privilege in others than the owner of the copyright to use the copyrighted material in a reasonable manner without his consent."[16] In 2010, 2012, 2015, and 2018, the Register and the Librarian correctly concluded that modifying the firmware in one's device in order to run lawfully acquired software is a fair use, falling squarely within Congress's intent to promote software interoperability.[17] The relevant law has not changed materially since the last rulemaking cycle, but we summarize it here.

[15] 17 U.S.C. § 107 ("The fair use of a copyrighted work . . . is not an infringement of copyright.").

[16] *Harper & Row, Publrs. v. Nation Enters., Inc.*, 471 U.S. 539, 549 (1985) (citations omitted).

[17] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. RM 2008-8, Final Rule, 75 Fed. Reg. 43825, 43828-29 (July 27, 2010) ("2010 Final Rule"); Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. 2011-7, Final Rule, 77 Fed. Reg. 65260, 65263-64 (October 26, 2012) ("2012 Final Rule"); Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. 2014-07, Final Rule, 80 Fed. Reg. 65944, 65952–53 (October 28, 2015)("2015 Final Rule"); Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. 2017-10, Final Rule, 83 Fed. Reg. 54010, 54020-21 (October 26, 2018)("2018 Final Rule").

a. The Purpose and Character of the Use

The first factor looks at whether the use of a copyrighted work is "more incidental and less exploitative in nature."[18] Where a user of software code is "not seeking to exploit or unjustly benefit from any creative energy that [the rightsholder] devoted to writing the program code," the first factor favors a finding of fair use.[19]

Over the years, a robust body of caselaw has developed regarding analysis and modification of the functional aspects of software. In *Sega v. Accolade*, the Ninth Circuit explained that research into the functional aspects of video game software was a legitimate purpose that favored a finding of fair use. Accolade reverse-engineered Sega's games to determine the requirements for compatibility with Sega's game consoles, in order to produce its own games.[20] The court found that Accolade's "direct use" of the code was done in service of a broader, favored purpose: building new, independently developed, compatible software.[21]

The Ninth Circuit expanded upon its reasoning in *Sony Computer Entertainment v. Connectix Corp*.[22] Connectix reverse-engineered the operating system software of the Sony Playstation console in order to create a platform that would allow games written for the Playstation to be played on personal computers.[23] The court held this to be a fair use, emphasizing that the innovation resulting from the creation of new platforms was favored under the first factor because it "afford[ed] [users] opportunities for game play in new environments."[24]

Jailbreaking promotes additional creativity and expands access to knowledge by encouraging more software development and making personal computing devices more useful.[25] As three Registers concluded in four prior proceedings, "the goal of jailbreaking is to allow the operating system on a device to interact with other programs, a favored purpose under the law."[26] Likewise, in the

---

[18] *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 544 (6th Cir. 2004) (quoting *Kelly v. Arriba Soft Corp.,* 336 F.3d 811, 818–19 (9th Cir. 2003)).

[19] *Id.* at 544.

[20] 977 F.2d 1510, 1514 (9th Cir. 1992), *as amended* (Jan. 6, 1993).

[21] *Id.* at 1522-23.

[22] 203 F.3d 596 (2000).

[23] *Id.* at 598-99.

[24] *Id.* at 606; *See also Bateman v. Mnemonics, Inc.*, 79 F.3d 1532, 1547 (11th Cir. 1996) (holding that "external factors such as compatibility" reduce the rightsholder's legal interest in the copyright and favor a finding of fair use).

[25] *See Sega*, 977 F.2d at 1522-23 (noting the public benefit that resulted from independent developers engaging in new creative expression).

[26] Section 1201 Rulemaking: Seventh Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendation of the Register of Copyrights 169 (October 2018), https://cdn.loc.gov/copyright/1201/2018/2018_Section_1201_Acting_Registers_Recommendation.pdf (2018 Register's Recommendation) ("[E]nabling a device's operating system to

legislative history of Section 1201(f), "Congress expressed a commitment to permit and encourage interoperability between independently created computer programs and existing programs," in order to "avoid hindering competition and innovation in the computer and software industry."[27]

Jailbreaking also allows device owners to better safeguard their privacy. For video streaming devices, this includes installing VPN software,[28] and removing code that sends tracking data to companies like Amazon, Google, and Apple.[29] Analyzing the first fair use factor, the Acting Register wrote in 2018 that protection of privacy "is a purpose for which circumvention may be warranted."[30]

Further, jailbreaking one's own device for personal use is noncommercial. As the Supreme Court noted in *Sony Corp. of America v. Universal Studios Inc.*, "private home use must be characterized as a noncommercial, nonprofit activity."[31] The Court held that without a demonstrable likelihood of harm to the copyright holder, a personal, noncommercial use of lawfully obtained works was fair use.[32] Likewise, video streaming device owners have a lawful copy of their device's firmware. Jailbreaking the device by modifying the firmware is noncommercial.[33]
Finally, jailbreaking is transformative: it does not "merely supersede[] the objects of the original

---

interoperate with other programs is a favored purpose under the first fair use factor."); *see also* Section 1201 Rulemaking: Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendation of the Register of Copyrights 188 (October 8, 2015), https://www.copyright.gov/1201/2015/registers-recommendation.pdf ("2015 Recommendation"); Recommendation of the Register of Copyrights, at 71-72, Section 1201 Rulemaking: Fifth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention (Oct. 12, 2012) ("2012 Recommendation"), http://www.copyright.gov/1201/2012/Section_1201_Rulemaking%20_2012_Recommendation.pdf; Recommendation of the Register of Copyrights in RM 2008-8, at 92, Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (June 11, 2010) ("2010 Recommendation"), www.copyright.gov/1201/2010/initialed-registers-recommendation-june-11-2010.pdf.

[27] 2010 Recommendation 92; *see also* 2012 Recommendation 71-72. In 2018, the Acting Register reiterated that statutory exemptions to the prohibition of Section 1201(a)(1) can illuminate Congress's intent with respect to triennial exemptions. 2018 Recommendation at 170 ("While proponents' requested exemption is not fully covered by the 1201(i), section 1201(i) reflects Congress's recognition that the protection of privacy is a purpose for which circumvention may be warranted under appropriate circumstances.").

[28] According to Jay Freeman, operator of the Cydia market for jailbroken iOS applications, access controls on the Apple TV prevent installing VPN software, even though substantially similar software is available for other iOS devices.

[29] Exhibit A, Statement of David Drager.

[30] 2018 Recommendation 170.

[31] 464 U.S. 417, 449-50 (1984).

[32] *Id.* at 454-56.

[33] *Cf. Sega*, 977 F.2d at 1522-24; *Connectix*, 203 F.3d at 606-07.

expression."[34] Modifying one's copy of a software program to render it compatible with other, independently created programs has been held to be a transformative purpose.[35] This finding is reinforced by decisions holding that the use of digital text and images for new purposes that are "different in purpose, character, expression, meaning, and message" from those of the copyright holder is transformative.[36]

While we recognize that the Office has questioned whether jailbreaking is transformative, we note that modifying device firmware to use it for lawful purposes that the manufacturer did not anticipate is, by definition, a new and different purpose and character of use. In any event, "even if jailbreaking is not considered transformative, 'the first factor may nonetheless favor fair use where, as here, the purpose and character of the use is "noncommercial and personal" and enhances functionality.'"[37]

In 2018, the Acting Register observed that "[n]othing in the record suggests that jailbreaking a voice assistant device is materially different in purpose and character from jailbreaking … other types of devices" for which exemptions have been granted.[38] The same is true for video streaming devices, which are functionally identical to smart TVs for which jailbreaking exemptions have been granted in two previous rulemakings.[39]

Because jailbreaking one's video streaming device to make its firmware interoperable with independently created software is personal, noncommercial, privacy-enhancing, transformative, and confers a public benefit, the first factor weighs in favor of a finding of fair use.

---

[34] *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 570 (1994).

[35] *Connectix*, 203 F.3d at 606-07.

[36] *Authors Guild, Inc. v. HathiTrust*, 755 F. 3d 87, 97 (2d Cir. 2014); *see also Authors Guild Inc. v. Google*, 804 F.3d 202, 214 (2d Cir. 2015) ("A transformative use is one that communicates something new and different from the original or expands its utility, thus serving copyright's overall objective of contributing to public knowledge."); *Perfect 10, Inc. v. Amazon.com, Inc.,* 508 F.3d 1146, 1165 (9th Cir. 2007)*; Kelly v. Arriba Soft Corp.*, 336 F.3d 811, 818-22 (9th Cir. 2003).

[37] 2018 Recommendation 169 (quoting 2015 Recommendation 188).

[38] *Id*.

[39] As the Register noted in 2018, the decision in *Oracle Am., Inc. v. Google LLC*, 886 F.3d 1179 (Fed. Cir. 2018) (*cert. granted*, 140 S. Ct. 520 (Nov. 15, 2019)) does not require a different conclusion. That case involved the creation of a derivative work of software that was *not* compatible with the plaintiff's original Java software, and that incompatibility was material to the Federal Circuit's conclusion that the challenged use was not transformative. *Id* at 1200. Jailbreaking a video streaming device, in contrast, expands the set of programs that are compatible with the device without rendering it incompatible with the original manufacturer's software.

b. The Nature of the Copyrighted Work

The second factor, the nature of the copyrighted work, also weighs in favor of fair use. In evaluating the second factor, courts look at the degree to which a work is creative or functional.[40] In *Sega*, the Ninth Circuit found that the second factor favors fair use where copying for reverse engineering purposes was necessary in order to understand software code's functional interoperability requirements.[41] As that court reasoned, "[i]f disassembly of copyrighted object code is per se an unfair use, the owner of the copyright gains a de facto monopoly over the functional aspects of his work—aspects that were expressly denied copyright protection by Congress."[42] The *Connectix* opinion further noted that "[i]f [copyright holder] Sony wishes to obtain a lawful monopoly on the functional concepts in its software, it must satisfy the more stringent standards of the patent laws."[43]

The firmware and operating system code on video streaming devices lies on the functional end of the spectrum, as it operates low-level functioning of the device rather than any audiovisual presentation. In the 2010, 2012, 2015, and 2018 rulemaking proceedings, relying in part on *Sega's* reasoning, the Register concluded that the second factor favors fair use for jailbreaking.[44] Noting that the second factor is "perhaps more important than usual in cases involving the interoperability of computer programs,"[45] the Register has noted that bootloaders and operating systems are largely functional works, and that "[a]s functional works, certain features are dictated by function and in order to interoperate with those works certain functional elements of those programs, elements that in and of themselves may or may not be copyrightable, must be modified."[46]

Thus, the second factor also favors a finding of fair use.

c. The Amount and Substantiality of the Portion Used

The third fair use factor examines the amount of the copyrighted work used in an effort to determine whether the "quantity and value of the materials used are reasonable in relation to the

---

[40] *Id.* at 1524 ("The second statutory factor, the nature of the copyrighted work, reflects the fact that not all copyrighted works are entitled to the same level of protection. The protection established by the Copyright Act for original works of authorship does not extend to the ideas underlying a work or to the functional or factual aspects of the work.").

[41] *Id.* at 1526.

[42] *Id.*; *see also Connectix*, 203 F.3d at 605 (finding the second statutory factor to "strongly favor" fair use where copying was necessary to disassemble and view the ideas contained within firmware).

[43] *Connectix*, 203 F.3d at 605.

[44] 2010 Recommendation 96; 2012 Recommendation 73; 2015 Recommendation 188; 2018 Recommendation 176.

[45] 2012 Recommendation 73.

[46] 2010 Recommendation 96.

purpose of the copying."[47] The use of an entire work does not preclude an activity from being a fair use.[48] The amount taken only need be "reasonable" and for a legitimate purpose.[49]

In *Connectix* and *Sega*, the Ninth Circuit found that copying a software program in its entirety in order to understand its functional components was necessary to achieving a favored purpose, and was therefore fair.[50] Similarly, in *Kelly v. Arriba Soft*, the court emphasized that copying anything less than an entire work would be insufficient in order to allow users to recognize images in a visual search engine.[51] In *Perfect 10,* the court concluded that Google's use of Perfect 10's images was reasonable in light of its purpose of communicating information to its users.[52] In both cases, the court found this copying to be fair use. And in *Authors Guild, Inc. v. Google*, in which the plaintiffs participated in the scanning and electronic storage of numerous books in their entirety, the court held that the copying was reasonable in light of its purpose.[53]

For jailbreaking video streaming devices, as with mobile computing devices, the portion of the firmware that must be permanently modified to accomplish a jailbreak is a very small proportion of the overall code. For example, the CheckRa1n jailbreak, which works on both iOS devices and current Apple TV models, involves just 9.2 megabytes of compiled code,[54] which is less than one percent of the size of the recent iOS installations on which tvOS is based.[55] Obtaining root access to an Amazon Fire TV Stick can be accomplished with minimal change to the code as well.[56]

In the previous rulemaking, the Acting Register noted that the third factor "has limited significance in the context of jailbreaking . . . in light of the *de minimis* nature of the modifications ultimately

---

[47] *Campbell*, 510 U.S. at 586-87.

[48] *Sega*, 997 F.2d at 1526.

[49] *Campbell*, 510 U.S. at 586.

[50] *Sega*, 977 F.2d at 1526 (9th Cir. 1992); *Connectix*, 203 F.3d at 605-06.

[51] 336 F. 3d at 820-21; *see also Field v. Google Inc.*, 412 F. Supp. 2d 1106, 1120-121 (D. Nev. 2006) (finding the third factor weighing in favor of neither party because, while Google copied entire pages in its web caching service, the amount used was necessary to the purpose).

[52] 508 F.3d at 1167-68.

[53] *Authors Guild v. Google, Inc.*, 804 F.3d 202, 221-22 (2d Cir. 2015).

[54] PANGU 8, "Checkra1n TV jailbreak for tvOS 14 – tvOS 13," https://pangu8.com/appletv/#checkrain (accessed Dec. 13, 2020).

[55] Chris Davies, "Apple iOS 14.2 released and it's huge – Here's what your iPhone gets," Slashgear (Nov. 5, 2020) https://www.slashgear.com/apple-ios-14-2-released-and-its-huge-heres-what-your-iphone-gets-05645916/ (accessed Dec. 13, 2020) (describing iOS as taking up 1.1 gigabytes).

[56] k4y0z, "[UNLOCK][ROOT][TWRP][UNBRICK] Fire TV Stick 2nd gen (tank)," XDA Developers (Mar. 3, 2019), https://forum.xda-developers.com/t/unlock-root-twrp-unbrick-fire-tv-stick-2nd-gen-tank.3907002/ (jailbreak code 8.2 megabytes in size).

made to the firmware to enable jailbreaking."[57] In short, the amount of code copied in the course of a jailbreak is necessary and reasonable. Thus, the third factor favors fair use, or is neutral.

d. Effect on the Market for the Copyrighted Work

The fourth factor considers the direct harms caused by a particular use on the market for or value of the work at issue, and the potential harm that might result from similar future uses.[58] Typically, courts require either a demonstration of actual harm or a likelihood that harm will result.[59] In *Sega*, the court emphasized that Accolade sought to become a legitimate competitor in the field of Genesis games and did not copy any of the elements of the Sega code that led to commercial success.[60] Moreover, consumers were likely to purchase more than one game, so sales of Accolade games would not directly foreclose Sega sales.[61] In *Connectix*, the court emphasized the transformative nature of the Connectix platform and concluded that any market harm to Sony would result from legitimate competition, not unfair copying.[62]

Jailbreaking video streaming devices does not foreclose sales of the device firmware. The firmware is sold along with the devices themselves, and not separately. A copy of the firmware is of no use without a device to run it. Firmware upgrades are not sold, but are made available to device owners as a free download. Thus, jailbreaking does not cause any proliferation of infringing copies, nor replace any sales.

Jailbreaking has not harmed sales of similar devices. For example, revenues from sales of smart TVs (and their accompanying firmware) have risen steadily since 2014, before the Librarian first granted an exemption for jailbreaking them, through 2020, and are predicted to continue rising.[63] In fact, the ability to jailbreak may *increase* the market value of a video streaming device. In 2014, when jailbreaks had not yet been created for the third-generation Apple TV, the resale value of second-generation devices for which a jailbreak was available remained unusually high.[64]

---

[57] 2018 Recommendation 171-72; *see also* 2015 Recommendation 189; *see also* 2010 Recommendation 97; 2012 Recommendation 73.

[58] *Campbell*, 510 U.S. at 590.

[59] *See, e.g.*, *Universal*, 464 U.S. at 451-52 (1984); *Campbell*, 510 U.S. at 590-92 (1994).

[60] 977 F.2d at 1523.

[61] *Id.*

[62] 203 F.3d at 607.

[63] H. Tankovska, "Smart TV market revenue in the United States from 2014 to 2025," Statista (Aug. 27, 2020), https://www.statista.com/statistics/781427/smart-tv-market-revenue-in-the-us/.

[64] Jeff Benjamin, "How to jailbreak iOS 5.3 on the Apple TV 2 untethered," iDB (Jan. 5, 2014), https://www.idownloadblog.com/2014/01/05/how-to-jailbreak-ios-5-3-on-the-apple-tv-2-untethered ("Be prepared to pay a markup for the [discontinued] Apple TV 2, because most sellers are aware of its value since it can be jailbroken.").

All four factors, including the important first and fourth factors, favor a finding of fair use. Jailbreaking video streaming devices for the purpose of installing lawfully acquired, interoperable software is a non-infringing fair use.

2. Circumvention Allows Device Owners Full Control of Their Devices, Enhancing Privacy and Extensibility.

The exemptions granted by the Librarian for jailbreaking mobile computing devices and smart TVs removed a cloud of legal uncertainty from device owners, spurring vibrant markets and communities of developers. Clarifying that the exemption class includes non-integrated video streaming devices would extend the positive changes wrought by the earlier exemptions. With the ability to jailbreak comes the ability to benefit from the hard work and expertise of independent developers in addition to the original manufacturer. Without a clarification or expansion to non-integrated devices, the availability of privacy enhancements, user control, and enhanced functionality on those devices would be limited by operation of the DMCA to what the manufacturer chooses to provide.

a. The Ban on Circumvention Limits the Functionality of Streaming Devices

The developer Kevin Bradley described the reasons for jailbreaking a video streaming device:

> Why jailbreak the AppleTV? For me the answer has always been the same, freedom. "This feature or behavior is missing from my favorite system on my TV or my phone, let me add it!" You may be motivated to tinker with your devices because you enjoy it and are passionate about contributing to a community that has such a rich history of drastically changing the ecosystem of a variety of Apple (or other companies) products. Our community had an App Store before Apple, we had copy and paste first, mobile notifier was a tweak Peter Hajas sold on the Cydia store before Apple hired him and a version of his solution became the de-facto way to receive notifications in iOS.[65]

Many significant and popular additions to a video streaming device can only be achieved by jailbreaking. For example, many users seek to replace the home screens generated by their streaming devices.[66] This requires jailbreaking, even on devices like the Fire TV that permit some sideloading of apps. As on other platforms, alternative "skins" or "themes" that change the look of the user interface are a highly sought-after feature.

Another popular use of jailbreaking is connecting one's video streaming device to other hardware and input devices. For example, the nControl app allows a user to connect a variety of game controllers and joysticks to an AppleTV.[67] Users also add a Web browser to their AppleTV, as the

---

[65] Kevin Bradley, "It's time to grow up," Scienceography (Aug. 24, 2019), https://sciencography.tumblr.com/post/187244563802/growup.

[66] Exhibit A, Statement of David Drager.

[67] nControl, AwkwardTV Wiki, https://wiki.awkwardtv.org/wiki/NControl (visited Dec. 13, 2020).

device doesn't come equipped with a browser.[68] Other programs that users add to their AppleTVs include support for an external broadcast TV tuner,[69] and a program called AirMagic that allows for remote control of an AppleTV from any device on a local network.[70] Some users also seek to install an alternative operating system on their devices, particularly Amazon Fire devices.[71]

Access controls also prevent developers from writing software that can run on multiple hardware platforms. According to developer Dan Aronson, "If [streaming video] devices allowed developers to 'root' them it could be possible for a developer community to build a universal environment . . . so the same software could be built to run on many different devices. This would enable software companies that are supporting these devices to radically reduce the cost to support platforms . . ."[72]

b. The Ban on Circumvention Limits Users' Control Over Their Privacy

As with voice assistants, smart TVs, and other personal computing devices, jailbreaking allows users to take greater control over their privacy. For example, although VPN apps are available in the Apple App Store, and even though the Apple TV uses the same basic networking code as other Apple devices, the access controls on the Apple TV do not allow the installation of a VPN. Jailbreaking allows an Apple TV owner to install a VPN and encrypt their network communications.[73] Jailbreaking also allows users to remove code that collects information about the user's activity and sends it to the manufacturer (such as Apple, Amazon, or Roku).[74]

3. The Nonexclusive Factors of Section 1201(a)(1)(C) Support Expanding The Exemption

a. The Availability for Use of Copyrighted Works

In considering this statutory factor, the Register examines whether "the availability for use of copyrighted works would be adversely affected by permitting an exemption."
Just as mobile computing devices and applications have continued their rapid growth despite (or because of) the existence of a jailbreaking exemption, the ability to jailbreak video streaming devices will have either no effect or a positive effect on the availability of copyrighted firmware and application software. With respect to smartphones, the Register previously concluded that jailbreaking to allow for interoperable software would increase the availability of applications "while simultaneously being unlikely to interfere with the availability of smartphone operating

---

[68] "Firefox," AwkwardTV Wiki, https://wiki.awkwardtv.org/wiki/Firefox (visited Dec. 13, 2020).

[69] "EyeTV," AwkwardTV Wiki, https://wiki.awkwardtv.org/wiki/EyeTV (visited Dec. 13, 2020).

[70] "AirMagic," http://wiki.awkwardtv.org/wiki/AirMagic

[71] Exhibit A, Statement of David Drager.

[72] Exhibit B, Statement of Dan Aronson.

[73] *See supra* note 29.

[74] Exhibit A, Statement of David Drager.

systems or other works currently being used or created for wireless communications devices."[75] The same holds true for video streaming devices.

Jailbreaking video streaming devices will not contribute to infringement of copyrighted entertainment media. To the extent that video streams are protected by digital rights management (DRM), such DRM is separate from the access controls in the bootloader and OS. For example, video streams from subscription-based services are often encrypted using Widevine technology, which requires licensed player software, and permission from the rightsholder, to decode.[76] Jailbreaking does not circumvent this type of access control, and the proposed expansion does not reach video DRM of the sort described in the audiovisual works exemptions granted in past cycles.[77]

b. The Availability for Use of Works for Nonprofit Archival, Preservation, and Education Purposes

The availability of firmware for nonprofit purposes will not be harmed by clarifying or expanding the jailbreaking exemption as to video streaming devices.

c. The Impact on Criticism, Comment, News Reporting, Scholarship or Research

A clarified or expanded exemption covering non-integrated video streaming devices will not have a significant impact on criticism, comment, news reporting, scholarship, or research, because most or all of the software that can be installed on a jailbroken device can also be installed on a smart TV for which an exemption is already available (and for which no objections were filed in this rulemaking cycle).

d. The Effect on the Market for, or Value of, Copyrighted Works

As we explained in our analysis of the fourth fair use factor, allowing users to jailbreak video streaming devices will have no negative impact on the actual market for the firmware on such devices. Instead, the proposed expansion is likely to stimulate the market for such works by permitting developers to create new applications for the devices that go beyond what the manufacturer has anticipated, thus making these devices—together with their copyrighted firmware—more attractive to consumers. The ability to develop and use independent applications, and the ability to control the functioning of those devices, increases the value of the devices and their firmware, and encourages still more application development.

e. Other Factors

Access controls on the installation and removal of software are sometimes used for anticompetitive purposes, such as preventing a competitor's applications from running on a device, or discouraging

[75] 2010 Recommendation 102.

[76] Widevine, https://widevine.com/ (accessed Dec. 13, 2020).

[77] *See, e.g.*, 2018 Recommendation 31-110.

users from switching away from the device manufacturer's applications.[78] The Office has recognized that Section 1201(a)(1) was not intended to lock out competition in the absence of copyright infringement.[79] Many of the manufacturers of video streaming devices produce video content of their own, giving them an incentive to block competitors' content from their devices. Manufacturers' desire to use access controls to keep competitors' video content and software off of video streaming devices should be given no weight in this rulemaking.

DOCUMENTARY EVIDENCE

Commenters are encouraged to submit documentary evidence to support their arguments or illustrate pertinent points concerning the proposed exemption. Any such documentary evidence should be attached to this form and uploaded as one document through regulations.gov.

[78] *See* Exhibit B, Statement of Dan Aronson.

[79] 2010 Recommendation 96-97 ("[W]hile a copyright owner might try to restrict the programs that can be run on a particular operating system, copyright law is not the vehicle for imposition of such restrictions, and other areas of the law, such as antitrust, might apply.").

Exhibit A

David Drager
Chief Technology Officer
XDA Developers
222 S Manoa Rd, Ste 100
Havertown, PA 19083

December 1st, 2020

To Whom It May Concern,

I am writing this letter in support of improving legal protections for streaming TV devices. My company is the sponsor for a community of programmers and developers, with a focus on mobile devices and specifically the Android operating system from Google. In this role, I have learned about the reasons someone might want to jailbreak or root a streaming TV device that they have purchased, and would like to share a few of those experiences with you in support of improved legal protections for those modifying their hardware devices.

Companies like Apple, Google, and Amazon sell an astounding amount of hardware in support of their software ecosystems. These devices implement access controls such as bootloader locking, software verification and signatures, and operating system locks in order to prevent owners from installing their own software or modifying their system.

There are many good reasons to support modifying these TV Streaming devices, like the Fire TV, Roku, and Apple TV:

- Allowing **security researchers** to evaluate the software for security holes, for example: an exploit that allows unknown 3rd parties to listen in on your device.
- Replacing the home screen for a different **user experience**.
- It is well known that everything you do on your streaming device, every show you watch, is tracked and analytics sent back to Amazon, Google and Apple. By rooting or jailbreaking these devices, you can disable this invasive tracking and **enhance your privacy**.
- You can **replace the voice assistant** now prevalent on many devices, such as switching between Google Assistant and Alexa.
- Installing an alternative or upgraded Operating System.

And many more. I would argue that improving the legal protections helps to promote freedom of choice as well as enhancing the security and usability of these streaming TV devices that are finding their way into more and more homes.

Please contact me if you have any questions or would like to discuss further.

Sincerely,

David Drager

Exhibit B

Statement of Dan Aronson in Support of Proposed Class 11

One of the challenges about proprietary media devices is that most of them have a unique way of writing software to interface with it. For example: Roku, Apple TV, iPhone, Samsung Smart devices and Amazon Fire stick each have a unique software environment. Many of the software environments are rudimentary and if they have ways to test or simulate they are all different.

If these devices allowed developers to "root" them it could be possible for a developer community to build a universal environment to so the same software could be built to run on many different devices. This would enable software companies that are supporting these devices to radically reduce the cost to support platforms (since instead of a dedicated team for each device, much more of the software and testing could be shared). The vendors themselves in general have no interest in that (since they are much more interested in vendor lock in). However, this is a clear place where the vendor interests don't necessarily coincide with the content creators or content distributors interest.