UNITED STATES COPYRIGHT OFFICE

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

Comments of the Electronic Frontier Foundation, Owners Rights Initiative, and the Association of Service and Computer Dealers International on Proposed Class 6 – Jailbreaking

ITEM A. COMMENTER INFORMATION

Electronic Frontier Foundation
Mitchell L. Stoltz
Corynne McSherry
Kit Walsh
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 40,000 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.

The Owners' Rights Initiative ("ORI") is an organization of over 20 companies and trade associations that have joined together to protect ownership rights in the United States.[1] We believe in the fundamental premise that **if you bought it, you own it**, and should have the right to sell, lend, or give away your personal property. ORI formed when the *Kirtsaeng v. Wiley* case was pending before the U.S. Supreme Court. We now are dedicated to preserving that holding, and making sure that it is not undermined in Congress, the executive branch, or the courts.

Association of Service and Computer Dealers International, Inc. ("ASCDI") is a trade group of more than 300 small-to-medium technology companies that buy, sell and service computer, telecom and other technical equipment and solutions.

[1] A list of ORI members can be found at http://ownersrightsinitiative.org/about/.

ITEM B. PROPOSED CLASS ADDRESSED

We submit these comments in support of Proposed Class 6. We ask the Office to expand the current exemption for jailbreaking personal computing devices to include similarly situated devices to which the same legal and factual analysis applies. In addition to smartphones and other mobile devices, the jailbreaking exemption should apply to voice assistant devices such as the Amazon Echo, Google Home, and Apple HomePod.

We propose to expand the existing exemption as follows:

> *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.***

This definition includes all devices that are subject to the current jailbreaking exemption, including smartphones, tablets, and smart watches. It expands on the current exemption in two respects: First, it adds an additional purpose for circumvention to the two existing purposes: to enable or disable hardware features of the smartphone or device. While the ability to enable or disable hardware features is inherent in the ability to install or remove software, making this permission explicit will clarify the regulation and further limit adverse impacts from the circumvention ban on the ability to customize devices. Second, the proposed definition includes multipurpose voice-controlled devices designed to be installed in a home or office in addition to those designed to be carried or worn.

This proposed class definition differs from the one EFF proposed in its Petition for a New Exemption regarding jailbreaking. We believe the definition above provides greater clarity.

ITEM C. OVERVIEW

Proposed Class 6 concerns jailbreaking personal computing devices. Jailbreaking describes practices that allow device users to install or remove software of their choosing. Jailbreaking or rooting require circumventing access controls imposed by the manufacturer that would otherwise prevent such modification. The Register of Copyrights has recommended, and the Librarian of Congress has enacted exemptions relating to jailbreaking in three previous triennial rulemaking cycles, beginning in 2010.

The 2010 and 2012 exemptions covered computer programs on "wireless telephone handsets."[2] In 2015, the Librarian enacted a broader exemption covering

> *[c]omputer programs that enable smartphones and portable all-purpose mobile computing devices 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 smartphone or device, or to permit removal of software from 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.*[3]

Besides broadening the category of devices subject to the exemption, the 2015 rule also acknowledged additional reasons to jailbreak computing devices: to *remove* unwanted software, and to enable timely operating system upgrades and security fixes.[4]

This year, as part of the newly instituted process for renewing previously granted exemptions, the Acting Register announced that she intends to recommend renewal of the 2015 jailbreaking exemption for the 2018-2021 period.[5]

The renewal and expansion of these exemptions reflects how the family of personal computing devices containing firmware access controls has evolved and become part of everyday life, along with the corresponding need to circumvent those access controls in order to adapt those devices to make them more efficient and effective.

[2] 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").

[3] 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").

[4] *Id.*; *see also* Section 1201 Rulemaking: Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendation of the Register of Copyrights 183 (October 8, 2015), https://www.copyright.gov/1201/2015/registers-recommendation.pdf ("2015 Recommendation") (noting evidence concerning the use of jailbreaking to install operating system upgrades).

[5] Exemptions to Permit Circumvention of Access Controls on Copyrighted Works, Docket No. 2017-10, Notice of Proposed Rulemaking, 82 Fed. Reg. 49550, 49553-54 (Oct. 26, 2017).

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

1. Voice Assistant Devices Are An Important Category Of Personal Computing Devices.

Voice assistant devices, also called "smart speakers," are a significant and growing category of personal computing devices. The first significant device in this market category was the Amazon Echo, introduced in 2014 and soon joined by a family of other Amazon devices.[6] It was followed in 2016 by the Google Home. Other devices were released or announced in 2017, including the Microsoft Invoke,[7] the Sonos One,[8] and the Apple HomePod, which the company plans to release in early 2018.[9] A market research firm predicts that 35.6 million Americans will use a voice assistant device in 2017, a 128.9 percent increase over 2016.[10] Estimates of the number of Amazon Echo devices installed before the 2017 winter holidays range from 7 million to 11 million.[11]

Voice assistant devices are small appliances designed to sit on a desk or tabletop. Their primary means of taking user input is through a microphone and voice recognition technology, although they generally include volume, action, and microphone off buttons.[12] Like smartphones and tablets, voice assistants have a broad and growing range of functions, including many kinds of information search and retrieval, voice communications, music streaming, and interacting with a wide variety of other devices, including lamps, thermostats, and home security systems.[13] The Echo devices can add items to shopping and to-do lists, set kitchen timers and recurring alarms, look up facts and unit conversions, recite curated news briefings, and control compatible home

[6] Jan Dawson, "Get ready, the smart speaker market pioneered by Amazon's Echo is about to get crowded," Recode (July 6, 2017), https://www.recode.net/2017/7/6/15929026/smart-speaker-market-voice-activated-assistant-amazon-echo-home-samsung-alibaba (accessed Dec. 15, 2017).

[7] Alex Cranz, "Microsoft Screams 'Me Too' With Cortana-Powered Rival to Amazon Echo and Google Home," Gizmodo (May 8, 2017) https://gizmodo.com/microsoft-screams-me-too-with-cortana-powered-rival-to-1795013201 (accessed Dec. 15, 2017).

[8] Nathan Ingraham, "Sonos One review: The best-sounding smart speaker you can buy, "Engadget (October 18, 2017), https://www.engadget.com/2017/10/18/sonos-one-review/ (accessed Dec. 15, 2017).

[9] Will Greenwald, "Apple HomePod," PCMag (June 7, 2017), https://www.pcmag.com/review/354139/apple-homepod (accessed Dec. 15,2017); HomePod, https://www.apple.com/homepod/ (accessed Dec. 15, 2017).

[10] Sarah Perez, "Amazon to control 70 percent of the voice-controlled speaker market this year," TechCrunch (May 8, 2017), https://techcrunch.com/2017/05/08/amazon-to-control-70-percent-of-the-voice-controlled-speaker-market-this-year/ (accessed Dec. 15, 2017).

[11] *Id.*

[12] Sascha Segan, "Amazon Echo (2017)," PCMag (Oct. 27, 2017), https://www.pcmag.com/review/356920/amazon-echo-2017 ("There are also physical volume, mic mute, and action buttons.") (accessed Dec. 15, 2017); Andrew Gebhart, "Google Home review: Google Home might be the virtual assistant for you," C|Net (May 25, 2017), https://www.cnet.com/products/google-home/review/ (describing the volume, action, and microphone mute controls on the Google Home) (accessed Dec. 15, 2017).

[13] Gebhart, *supra* n. 13; Segan, *supra* n. 13 (describing device features).

appliances.[14]

Streaming music is one function among many on these devices. They do not ordinarily store music, video, or images, except perhaps in buffers that assist streaming.[15] According to Apple, "HomePod isn't just great at playing your music. It's also a helpful home assistant for everyday household questions and tasks. And it's a hub for controlling your smart home accessories — from a single light bulb to the whole house — with the power of your voice."[16] A review of the Echo concluded that "the Echo is more than a music streamer, just as an iPhone is more than a telephone."[17] And a market analyst observed that "[o]lder millennials are the core users of virtual assistants, mainly due to their demand for *functionality over entertainment*."[18]

Some manufacturers, including Amazon, allow third-party developers to write new applications (sometimes called "Skills") for the devices, in a similar manner to smartphone apps. Others, including Apple, will not allow third-party applications without jailbreaking.[19]

Like smartphones and tablets, voice assistant devices perform functions that are deeply personal and vary widely between users. The intimacy of voice interactions in the home creates a strong demand for customization. It also raises significant security and privacy concerns. Voice assistant devices capture and buffer ambient sound continuously, including conversations, and transmit those recordings to the manufacturer's servers when a trigger word such as "Alexa" is heard.[20] Control over lights, home security, etc. also raises obvious security concerns.[21] More broadly, any device designed to listen continuously within a home and to interact via the Internet

[14] Ry Crist, "Amazon Echo Show Review: It's more Echo than Show,") C|Net (Oct. 26, 2017), https://www.cnet.com/products/amazon-echo-show/review/ (accessed Dec. 15, 2017) ("Crist").

[15] None of the devices described in these comments are advertised as having a local media storage capability.

[16] "HomePod," https://www.apple.com/homepod (accessed Dec. 15, 2017).

[17] Ry Crist and David Carnoy, "Amazon Echo review: The smart speaker that can control your whole house," C|Net (October 26, 2017), https://www.cnet.com/products/amazon-echo-review/ (accessed Dec. 15, 2017).

[18] "Alexa, Say What?! Voice-Enabled Speaker Usage to Grow Nearly 130% This Year," E-Marketer (May 8, 2017), https://www.emarketer.com/Article/Alexa-Say-What-Voice-Enabled-Speaker-Usage-Grow-Nearly-130-This-Year/1015812 (accessed Dec. 15, 2017) (emphasis added).

[19] Oscar Raymundo, "The HomePod needs to run third-party iOS apps. Here's why," Macworld (Aug. 25, 2017), https://www.macworld.com/article/3217018/consumer-electronics/the-homepod-needs-to-run-third-party-ios-apps-heres-why.html (accessed Dec. 15, 2017).

[20] Tim Moynihan, "Alexa and Google Home Record What You Say. But What Happens To That Data?," Wired (Dec. 5, 2016), https://www.wired.com/2016/12/alexa-and-google-record-your-voice/ (accessed Dec. 15, 2017) ("Moynihan").

[21] Notably, Amazon also sells an electronic home door lock, Internet-controlled and integrated into Amazon's other services. Elizabeth Weise, "New Amazon Key lets the delivery driver leave packages inside the front door," USA Today (Oct. 25, 2017), https://www.usatoday.com/story/tech/news/2017/10/25/new-amazon-key-lets-delivery-driver-leave-packages-inside-front-door/796780001/ (accessed Dec. 15, 2017).

raises a possibility of unwanted eavesdropping, whether human or algorithmic.[22]

Like smartphones, tablets, and wearable computing devices, voice assistants contain fundamental computer programs that start up the device, control the hardware, and allow the running of other programs. These low-level programs are known as firmware, operating systems, and bootloaders. These comments will refer to them collectively as firmware. Voice assistants from Amazon and Google run variants of the GNU/Linux operating system, the same operating system that runs on billions of other Internet-connected devices and forms the basis of the Android operating system for mobile devices.[23] The Apple HomePod runs iOS, the same operating system that runs on iPhone and iPad devices.[24]

While voice control can be built into other types of hardware, including desktop and laptop computers, voice assistant devices are designed *primarily* for voice input rather than touch, keyboard, button, or other modes of input. And voice assistant devices are distinguishable from game consoles and television set-top boxes by the broad range of applications they support.

2. The Technological Protection Measures and Methods of Circumvention: Linux "root" Privileges, Cryptographic Verification of Software, and Locked Bootloaders.

The firmware in voice assistant devices contains technological measures that restrict the ability to add or remove software from the device, and to enable or disable particular features of the hardware. They also contain measures that make the firmware resistant to modification or replacement.

a. GNU/Linux: Lack of Access to Root Privileges

The firmware on most voice assistant devices is a variant of GNU/Linux. 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.[25] When those access controls are enabled, modifying the functioning of the device requires root, or superuser, access to the device.[26] Analyses of Amazon Echo[27] and Google Home[28] reveal that neither vendor grants root

[22] Last year, Amazon agreed to hand over stored recordings captured by an Echo device in a home to police as part of a criminal investigation. Christina Warren, "Amazon Agrees to Hand Over Data in Echo Murder Case," Gizmodo (Mar. 17, 2017), https://gizmodo.com/amazon-agrees-to-hand-over-data-in-echo-murder-case-1793039360 (accessed Dec. 15, 2017).

[23] Ike Clinton, Lance Cook, and Dr. Shankar Banik, "A Survey of Various Methods for Analyzing the Amazon Echo," *available at* https://www.slideshare.net/IkeClinton/a-survey-of-various-methods-for-analyzing-the-amazon-echo (accessed Dec. 15, 2017) ("Clinton et al.").

[24] Raymundo, *supra* n. 19.

[25] James Morris, "Overview of Linux Kernel Security Features," The Linux Foundation (July 11, 2013), https://www.linux.com/learn/overview-linux-kernel-security-features (accessed Dec. 15, 2017).

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

[27] Clinton et al., *supra* n. 23.

access to the owner or user of the device, and that obtaining it requires modifying or replacing the access controls on the device. In one analysis, a researcher connected a second computer to contact points on the Echo's lower surface, determined the function of those points, and used them to install new software that overwrites the Echo's Linux security system.[29]

Entrepreneur and cloud computing pioneer Todd Troxell submits this description of the access controls on voice assistants:

> In order to be able to install unapproved applications, a device owner may need the ability to install custom firmware on the device, to modify the bootloader, to circumvent DRM and encryption, to obtain root access or otherwise work around filesystem and operating system access privileges. They will need some form of write access to the device and currently all such access is mediated by entirely by the device manufacturers. These are all things that are possible but currently restricted by our inability to circumvent protection mechanisms on these devices.[30]

b. iOS on the Apple HomePod: Cryptographic Verification of All Software

The Apple HomePod runs iOS,[31] the same operating system that runs on iPhone and iPad devices already subject to a §1201(a)(1) exemption. Devices that run iOS are subject to severe restrictions on the loading, running, and deletion of software. iOS contains cryptographic verification that prevents any application from running on a device unless it bears a digital signature from Apple.[32] This restriction means that new software can normally only be loaded on a device through Apple's iTunes Store or another Apple-provided channel. It also contains cryptographic checks at various levels of the software stack that prevent modification or replacement of the operating system itself.[33]

[28] iFixit, Google Home Teardown (Nov. 7, 2016), https://www.ifixit.com/Teardown/Google+Home+Teardown/72684 (accessed Dec. 15, 2017).

[29] Clinton et al., *supra* n. 23.

[30] Exhibit A, Statement of Todd Troxell, at 2.

[31] Raymundo, *supra* n. 19.

[32] Apple Inc., *iOS Security—iOS 10*, at 19 (Mar. 2017), https://www.apple.com/business/docs/iOS_Security_Guide.pdf ("Apps provided with the device . . . are signed by Apple. Third-party apps must also be validated and signed using an Apple-issued certificate.") (accessed Dec. 15, 2017).

[33] *Id.* at 5 ("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.").

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

1. Jailbreaking Voice Assistant Devices Is Non-Infringing

Jailbreaking involves modifying the firmware on one's device, potentially creating a derivative work. Nonetheless, it does not infringe copyright, because it is a fair use.[34] 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."[35] In 2010, 2012, and 2015, 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.[36] The relevant law has not changed materially since 2015, but we summarize it here.

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."[37] 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.[38]

Over the years, a robust body of caselaw has developed regarding the 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.[39] 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.[40]

The Ninth Circuit expanded upon its reasoning in *Sony Computer Entertainment v. Connectix Corp*.[41] 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.[42] 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

[34] 17 U.S.C. § 107 ("The fair use of a copyrighted work . . . is not an infringement of copyright.").
[35] *Harper & Row, Publrs. v. Nation Enters., Inc.*, 471 U.S. 539, 549 (1985) (citations omitted).
[36] 2010 Final Rule at 43828-29; 2012 Final Rule at 65263-64; 2015 Final Rule at 65952.
[37] *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)).
[38] *Id.* at 544.
[39] 977 F.2d 1510, 1514 (9th Cir. 1992), *as amended* (Jan. 6, 1993).
[40] *Id.* at 1522-23.
[41] 203 F.3d 596 (2000).
[42] *Id.* at 598-99.

because it “afford[ed] [users] opportunities for game play in new environments.”[43]

As two Registers concluded in three 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.”[44] Likewise, in the 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.”[45]

Jailbreaking is transformative: it does not “merely supersede[] the objects of the original expression.”[46] Copying and modification of software to render it compatible with other, independently created software has been held to be a transformative purpose.[47] 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.[48]

While we recognize that the Office has previously questioned whether jailbreaking is transformative, we note that modifying device firmware to use it for lawful purposes that the manufacturer did not anticipate or approve is, by definition, a new and different “purpose and character” of use. In any event, the Register has recognized that jailbreaking is likely to be a fair use “even if this use is not considered transformative in nature.”[49]

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

[43] *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).

[44] 2015 Recommendation 188; *see also* 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”), *available at* 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”), *available at* www.copyright.gov/1201/2010/initialed-registers- recommendation-june-11-2010.pdf;

[45] 2010 Recommendation 92; *see also* 2012 Recommendation 71-72.

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

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

[48] *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).

[49] 2015 Recommendation 188.

characterized as a noncommercial, nonprofit activity," even where the use involved lawfully obtained copies of commercially distributed works.[50] The Court held that without a demonstrable likelihood of harm to the copyright holder, a personal, noncommercial use was fair use.[51] Likewise, voice assistant device owners who jailbreak do not do so for profit, but to enhance, personalize, and secure their devices.[52]

In addition, jailbreaking promotes additional creativity and expands access to knowledge by encouraging more software development and expanded functionality.[53] As discussed further below, jailbreaking allows voice assistant users to run applications that fall outside of any categories anticipated by the manufacturer, including applications that enhance the user's control over their privacy. Because jailbreaking one's voice assistant device to make its firmware interoperable with independently created software is transformative, personal, noncommercial, and confers a public benefit, the first factor weighs in favor of a finding of fair use.

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.[54] 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.[55] 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."[56] 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."[57]

In the 2010, 2012, and 2015 rulemaking proceedings, relying in part on *Sega's* reasoning, the Register concluded that the second factor favors fair use.[58] Noting that the second factor is "perhaps more important than usual in cases involving the interoperability of computer

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

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

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

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

[54] *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.").

[55] *Id.* at 1526.

[56] *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).

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

[58] 2010 Recommendation 96, 2012 Recommendation 73; 2015 Recommendation 188.

programs,"[59] the Register noted in 2012 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."[60]

The Federal Circuit's 2014 holding in *Oracle v. Google* regarding fair use of software interfaces is consistent with the Registers' reasoning in past rulemakings. The court noted that some elements of computer programs are "dictated by considerations of efficiency or other external factors" and held that "where the nature of the work is such that purely functional elements exist in the work and it is necessary to copy the expressive elements in order to perform those functions, consideration of this second factor arguably supports a finding that the use is fair."[61]

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 purpose of the copying."[62] The use of an entire work does not preclude an activity from being a fair use.[63] The amount taken only need be "reasonable" and for a legitimate purpose.[64]

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.[65] 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.[66] In *Perfect 10,* the court concluded that Google's use of Perfect 10's images was reasonable in light of its purpose of communication information to its users.[67] 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, the court held that the copying was reasonable in light of its purpose.[68]

For jailbreaking, the amount of code that must be copied and modified varies depending on the device and firmware. In most cases, 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,

[59] 2012 Recommendation 73; 2010 Recommendation 95.
[60] 2010 Recommendation 96.
[61] *Oracle America, Inc. v. Google Inc.*, 750 F. 3d 1339, 1375 (Fed. Cir. 2014).
[62] *Campbell*, 510 U.S. at 586-87.
[63] *Sega*, 997 F.2d at 1526.
[64] *Campbell*, 510 U.S. at 586.
[65] *Sega*, 977 F.2d at 1526 (9th Cir. 1992); *Connectix*, 203 F.3d at 605-06.
[66] 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).
[67] 508 F.3d at 1167-68.
[68] *Authors Guild v. Google, Inc.*, 804 F.3d 202, 221-22 (2d Cir. 2015).

the Yalu 102 jailbreak for iOS 10.2 involves just 8 megabytes of compiled code, [69] which is less than one percent of the size of recent iOS installations.[70] Obtaining root access to an Amazon Echo can be accomplished with minimal changes as well.[71]

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. In prior rulemakings, the Register noted that the third factor is "of limited relevance" in this context.[72]

d. Effect on the Market for the Copyrighted Work

The fourth factor considers the direct harms caused by a particular use on the market or value of the work at issue, and the potential harm that might result from similar future uses.[73] Typically, courts require either a demonstration of actual harm or a likelihood that harm will result.[74] 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.[75] Moreover, consumers were likely to purchase more than one game, so sales of Accolade games would not directly foreclose Sega sales.[76] 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.[77]

By the same token, jailbreaking voice assistant devices does not foreclose sales of the device firmware. The firmware for voice assistant devices is sold along with the devices themselves, 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 other devices. An exemption class for jailbreaking smartphones has been in place since 2010.[78] Since that time, smartphone sales have continued to grow rapidly.[79]

[69] "Yalu 102", https://github.com/kpwn/yalu102 (Beta 7) (accessed Dec. 15, 2017).

[70] George Tinari, "No, iOS 9 probably isn't too big for your iPhone," Cult of Mac (Sep. 16, 2015), https://www.cultofmac.com/389120/ios-9-not-too-big/ (accessed Dec. 15, 2017).

[71] Clinton et al., *supra* n. 23.

[72] 2015 Recommendation 189; *see also* 2010 Recommendation 97; 2012 Recommendation 73.

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

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

[75] 977 F.2d at 1523.

[76] *Id.*

[77] 203 F.3d at 607.

[78] *See supra* n.2.

[79] "In 2016, the number of smartphones sold to consumers stood at around 1.5 billion units, a significant increase from the 680 million units sold in 2012." Statista, "Number of smartphones sold to end users worldwide from 2007 to 2016 (in million units)," https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/ (accessed Dec. 15, 2017).

All four factors, including the important first and fourth factors, favor of a finding of fair use. Jailbreaking voice assistant 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 since 2010 for jailbreaking phones and other mobile computing removed a cloud of legal uncertainty from device owners, spurring vibrant markets and communities of developers. Broadening the exemption class to include voice assistant 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 fear of circumvention liability. Rejecting an expansion would mean that privacy enhancements, user control, and enhanced functionality would be limited by operation of the DMCA to what the manufacturer chooses to provide.

a. The Ban on Circumvention Limits the Functionality of Voice Assistant Devices.

Voice assistant devices, though versatile, are limited in their functionality by manufacturer-imposed restrictions on software installation and modification. For example, while developers of "Skills" (applications) for the Amazon Echo can cause the device to read out information compiled from the Internet, they cannot vary the speed at which the text is read.[80] Engineer Todd Troxell describes the limitations of an Amazon Skills developer without access to jailbreaking:

> Currently all power for developers like me to innovate on Alexa is bestowed by Amazon. I would love to be give my DailyZen application some interactive functionality but because it is a Flash Briefing skill it can only do one thing-output a daily quote. My only option is to make a second application and hope my users install it. This new application would not be able to issue Flash Briefings so users would have to have multiple applications installed. On top of this I've gotten complaints that my application reads these Zen quotes too fast and does not leave room for a user to reflect before moving on. There is no way to pause or slow down a reading on Alexa.[81]

Obtaining root (superuser) access to a device by jailbreaking it allows the device's owner to add functionality not anticipated by the manufacturers.

New features created by the jailbreaking community are often adopted by the manufacturers themselves. Many popular features of the iPhone began as features available only on jailbroken phones before being adopted by Apple.[82] Voice assistant devices will benefit from this dynamic.

[80] Exhibit A, Comments of Todd Troxell, at 1.

[81] *Id.*

[82] Joe Rossignol, *15 jailbreak tweaks that iOS 8 made obsolete*, iDownloadBlog (Jun. 3, 2014), http://www.idownloadblog.com/2014/06/03/15-jailbreak-tweaks-that-ios-8-made-obsolete/ (accessed Dec. 15, 2017); Luke Villapaz, *Apple iOS 8 Features Make Several Jailbreak Tweaks*

The ability to jailbreak without legal uncertainty under § 1201(a)(1) would also allow device owners to fix security vulnerabilities or disable vulnerable features *before* the manufacturer gets around to addressing those issues.

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

Voice assistant devices raise a notable privacy risk as "always-on" devices designed to listen continuously to ambient sound for possible commands.[83] Some are also equipped with cameras.[84] In general, they are designed to transmit audio commands over the Internet to the manufacturer's servers for interpretation. They may also report other sensitive information to the manufacturer, including data from "smart home" devices like thermostats and lamps that interface with the voice assistant.

While manufacturers offer basic privacy tools, such as a button that disables the microphone, jailbreaking allows for more fine-grained control over the information collected and transmitted by a voice assistant. For example, jailbreaking allows a user to install firewall software that blocks certain network requests to the device or prevents the transmission of particular information. Jailbreaking also enables a user to adjust GNU/Linux permissions at the same degree of specificity as the manufacturer. This allows, for example, shutting off the microphone or camera at particular times of day, and limiting access to particular applications or hardware features based on criteria of the user's choosing.

c. The Ban on Circumvention Leads To Early Obsolescence Of Voice Assistant Devices.

Current voice assistant devices connect to a manufacturer's servers to perform voice recognition and retrieve information. Thus, if the manufacturer shuts down its servers or ceases to support a particular device or model, the device can become useless, even though the device *hardware* will often have a much longer useful lifespan.[85] The end of manufacturer support also means that a

Obsolete With Custom Keyboards, Interactive Notifications And Touch ID, International Business Times (Jun. 3, 2014), http://www.ibtimes.com/apple-ios-8-features-make-several-jailbreak-tweaks-obsolete-custom-keyboards-interactive-1593829 (accessed Dec. 15, 2017).

[83] Moynihan, *supra* n. 20.

[84] Crist, *supra* n. 14.

[85] Software architect Bill Sempf recounts his experience with hardware obsolescence enforced by access controls:

> This was the first decent smartwatch, and had a thriving developer community. But, they were bought by Fitbit. The watches depend on a service provided by Pebble to function, but those servers could go away anytime. (https://blog.getpebble.com/2016/12/07/fitbit/) So millions of $300 watches, just worthless. BUT, Pebble left the bootloader unlocked. So now there is an open source backend and matching firmware, called Rebble (https://rebble.io/) that will keep Pebble watches working. You can't do that with an Echo - Amazon won't let

device will not receive security updates, which could leave it insecure in the face of known vulnerabilities.

Without the ability to jailbreak, a customer's only recourse is to acquire a new device. Electronics waste is a serious and growing environmental problem that is alleviated by the ability to update device firmware.[86] Jailbreaking allows a user to repurpose an otherwise obsolete device, avoid unwanted software updates from the manufacturer, or to reconfigure a device to connect to a new server. The ability to jailbreak a device makes it less susceptible to obsolescence, and thus more valuable.

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 voice assistant 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 systems or other works currently being used or created for wireless communications devices."[87] The same holds true for voice assistant devices.

Jailbreaking voice assistant devices will not contribute to infringement of copyrighted entertainment media. Voice assistant devices stream audio from remote sources and do not store media locally (except possibly in a temporary cache to aid in playback).[88] To the extent that audio streams are protected by digital rights management (DRM), such DRM is separate from the access controls in the bootloader and OS. For example, audio streams from Apple Music and Spotify are sent encrypted, and then decrypted by a specific application on the device. Jailbreaking does not circumvent this type of access control, and the proposed expansion does not reach streaming music DRM.

> you. Without a "jailbreak", when Amazon moves on to the next format the first generation Echos will just be trash, literally.

Exhibit B, Statement of Bill Sempf.

[86] *E-waste is the Toxic Legacy of our Digital Age*, IFIXITORG, http://ifixit.org/ewaste (accessed Dec. 15, 2017).

[87] 2010 Recommendation 102.

[88] None of the devices reviewed by the commenters were advertised as including a local media storage capability.

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 expanding the jailbreaking exemption to cover voice assistant devices. Jailbreaking a voice assistant could enable the device to be used for capturing and preserving an audio record under the control of the device owner, with voice control over the recording functions.

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

Device manufacturers who use access controls to limit the use of apps often exclude third-party apps based on their content. For example, Apple will not approve apps containing "content that is offensive, insensitive, upsetting, intended to disgust, or in exceptionally poor taste" for sale in its app store, which means apps with content that Apple deems objectionable cannot be installed on iOS devices without jailbreaking.[89] Manufacturers sometimes prevent the installation of apps at the request of repressive governments. This year, Apple removed virtual private network apps, a commonly used type of privacy-enhancing software, from its app store in China at the request of the Chinese government.[90] An expanded exemption permitting jailbreaking of voice assistant devices will allow users to install, use, study, and comment upon software regardless of its content, avoiding censorship by companies and governments.

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 voice assistant 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 on voice assistant devices, 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 users from switching away from the device manufacturer's applications. The Office has recognized that Section 1201(a)(1) was not intended to lock out competition in

[89] "App Store Review Guidelines," https://developer.apple.com/app-store/review/guidelines/ (accessed Dec. 15, 2017).

[90] Jon Russell, "Apple removes VPN apps from the App Store in China," TechCrunch (July 29, 2017), https://techcrunch.com/2017/07/29/apple-removes-vpn-apps-from-the-app-store-in-china/ (accessed Dec. 15, 2017).

the absence of copyright infringement.[91] Manufacturers' desire to use access controls to keep competitors' software, such as rival music streaming services, off of voice assistant devices should be given no weight in this rulemaking.

4. The Librarian Should Clarify The Exemption Class For All Users By Explicitly Including The Enabling and Disabling of Hardware Features.

The existing exemption for jailbreaking exempts the installation of new or lawfully modified software on a mobile device from the prohibition of § 1201(a)(1). Installing new or modified software on a device inherently includes the ability to activate or deactivate features of the device hardware such as microphones, cameras, and wireless interfaces. However, because of the importance of this ability, particularly to protect user privacy and security, we request that the Office recommend including that purpose explicitly in the exemption.

[91] 2010 Recommendation at 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

To: Office of Copyright

Todd Troxell
San Jose CA
https://www.linkedin.com/in/toddtroxell/

I am an entrepreneur and inventor based in San Jose, California with 20 years of experience in building technologies, products, teams and startups. I helped lay the groundwork for some modern cloud technologies while working at Rackspace and I've helped move technology forward for multiple early stage companies including as a founder and chief technology officer. My creations have been core revenue generators for startups and Fortune 500s. I have created applications for the Amazon Alexa platform called "skills". One of them is called DailyZen and it plays a mindful quotation to the user each day. It is fairly popular with about 10,000 users.

The voice assistant space is very interesting to me in its ability to augment the way we interact with computers. It feels inevitable to me that voice interaction will continue to spread to the technologies we rely on every day. Much in the way the invention of the mouse and graphical user interface changed the way we use modern computers, voice interaction has the opportunity to dramatically augment and make these devices more accessible.

The power to innovate on these platforms is artificially restrained by the inability of device owners to inspect, modify and especially to install 3rd party applications which have not been approved by the manufacturer. Much like mobile App Stores, this ecosystem lends itself to supporting exclusively the interests of the manufacturers of these devices and to restrict anyone else from creating value on a level playing field.

Currently all power for developers like me to innovate on Alexa is bestowed by Amazon. I would love to be give my DailyZen application some interactive functionality but because it is a Flash Briefing skill it can only do one thing- output a daily quote. My only option is to make a second application and hope my users install it. This new application would not be able to issue Flash Briefings so users would have to have multiple applications installed. On top of this I've gotten complaints that my application reads these Zen quotes too fast and does not leave room for a user to reflect before moving on. There is no way to pause or slow down a reading on Alexa.

This was my personal development experience but far more concerning is our inability to work outside the very narrowly crafted APIs that Amazon has created. Every interaction is precisely scripted and while the manufacturers tried to accommodate as many developers as possible the current ecosystem lends itself more strongly to ease of use than power. Applications can not interact with each other and for example if I wanted to create something to filter curse words from all applications it would not be possible without gaining access to the system behind the official APIs.

Perhaps most critically welcoming a device like this into our homes has some interesting security concerns. For my own privacy rather than take Amazon's word for it, I would prefer to be able to monitor what recordings Alexa sends back to Amazon. Currently we must trust them, and it's not because the technology to intercept to this stream is impossible or even very difficult to create.

In order to be able to install unapproved applications, a device owner may need the ability to install custom firmware on the device, to modify the bootloader, to circumvent DRM and encryption, to obtain root access or otherwise work around filesystem and operating system access privileges. They will need some form of write access to the device and currently all such access is mediated by entirely by the device manufacturers. These are all things that are possible but currently restricted by our inability to circumvent protection mechanisms on these devices.

I support enthusiastically the effort to create an exception for this class of device and I'd be happy to share anything else that might help you make a decision.

Todd Troxell

Exhibit B

Comments of Bill Sempf in Support of Proposed Class 6
December 18, 2017

My name is Bill Sempf. In 1992, I was working as a systems administrator for The Ohio State University, where I formalized my career-long association with internetworking. While working for one of the first ISPs in Columbus in 1995, I built the second major web-based shopping center, Americash Mall, using Cold Fusion and Oracle. My focus started to turn to security around the turn of the century. Internet-driven viruses were becoming the norm by this time, and applications were susceptible to attack like never before. In 2003, I wrote the security and deployment chapters of the often-referenced Professional ASP.NET Web Services for Wrox, and began my career in penetration testing and threat modeling with a web services analysis for the State of Ohio.

Currently, I work as a security-minded software architect specializing in the Microsoft space. I recently designed a global architecture for a telecommunications web portal, modeled threats for a global travel provider, and provided identity policy and governance for the State of Ohio. Additionally, I publish technical books, with the latest being “Windows 8 Application Development with HTML5 for Dummies.”

In this new world of internet connected appliances, we have forgotten the concept of ownership. Devices like voice-controlled home assistants, when bought with pre-loaded services, don't allow the person who bought the device to actually own it. Once the services have changed, and the manufacturer doesn't see fit to update the device any longer, it just becomes another piece of technological trash. With root access to these devices, like we have to most phones and personal computers today, a new life can be found for these devices. An example comes from the Pebble smartwatch. This was the first decent smartwatch, and had a thriving developer community. But, they were bought by Fitbit.

The watches depend on a service provided by Pebble to function, but those servers could go away anytime. (https://blog.getpebble.com/2016/12/07/fitbit/) So millions of $300 watches, just worthless. BUT, Pebble left the bootloader unlocked. So now there is an open source backend and matching firmware, called Rebble (https://rebble.io/) that will keep Pebble watches working. You can't do that with an Echo - Amazon won't let you. Without a "jailbreak", when Amazon moves on to the next format the first generation Echos will just be trash, literally.

This is aside from the real security considerations of allowing members of the community to test features of the of the device to assure that they perform as specified.