UNITED STATES COPYRIGHT OFFICE

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

Initial Comment of Electronic Frontier Foundation, Owners' Rights Initiative, and Association of Service and Computer Dealers International Regarding Class 7: Repair, Diagnosis, and Modification

December 18, 2017

ITEM A. COMMENTER INFORMATION

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.

Contact Information

Kit Walsh, Staff Attorney
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
415 436 9333
kit@eff.org

ITEM B. PROPOSED CLASS ADDRESSED

Proposed Class 7: Computer Programs—Repair

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

ITEM C. OVERVIEW

Software-enabled devices are ubiquitous in modern life. One consequence of this phenomenon has been limiting the ability of device owners to repair, diagnose, or modify their property, thanks in part to restrictions imposed by Section 1201(a)(1).

As a consequence, competition and innovation are reduced in the markets for repair parts, alternative software, and peripherals that could interoperate with software-enabled devices. TPMs enforce ignorance over the inner workings of the device in your life, inhibiting learning as well as important investigations into privacy and safety risks.

Copyright law was never intended to enforce ignorance of a work when you own a copy of that work. An exemption is necessary to prevent it from doing so.

Relevant devices include, but are not limited to:

- The "Internet of Things" – devices connected to the Internet that primarily have a physical function or sense the physical world.
- Appliances – computerized refrigerators, toasters, and temperature control systems.
- Computer peripherals – such as printers, 3D printers, displays, or human interface devices.
- Computers, storage devices, and playback devices – such as desktop and laptop computers, tablets, wearable computers, phones, video game consoles, and media devices.
- Toys – computerized dolls or other toys.
- Vehicles – computerized vehicles for land, water, or air use.
- Environmental automation systems – for the home or office, controlling climate, doors, or elevators.

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

The most common TPMs are encryption applied to the software or data compilation, or passwords or handshakes by which access is restricted. One common form of TPM requires such authentication before firmware may be read out of a device, or "dumped" to the user's computer. Such measures can be bypassed by brute force techniques, use of leaked credentials, or analysis of the electrical properties of a computer memory itself.

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

Repair and tinkering includes a variety of activities that require an exemption to alleviate the adverse effects of the ban on circumvention:

- Repair of defects, damage, wear, or other issues affecting the physical device or software.
- Diagnosis of unintended or undesired behavior, including behavior such as privacy intrusions or planned obsolescence that are intended by the manufacturer but objectionable to the customer.

- Modification in order to add new features, load the software of one's choice, disable undesired functionality, or customize the operation of the device to one's preferences.

The Copyright Office has documented examples in its 1201 Report of TPMs interfering in device diagnosis and report.[2]

In addition, further examples of adverse effects on various technologies are documented below.

A. Exemplary Uses

1. Philips Hue Lighting System Modification

Philips Hue, a wireless lighting system designed by Philips, allows users to control a range of smart light bulbs using switches, sensors, and a software application.[3]

Individuals have published modified firmware on the web that allows users to connect the Philips Hue to an LED light and other monochromatic bulbs rather than Philips manufactured bulbs.[4]

To modify the firmware, Philips Hue users must bypass the encryption which restricts the ZigBee Light Link software that allows these devices to communicate.[5] The decryption key used to encrypt the Zigbee Light Link is available online.[6]

These modifications are becoming increasingly necessary as some appliance companies, including Philips, have recently engaged in anti-competitive DRM practices.[7] In 2015, Phillips released a firmware update which severely limited the bulbs functionality, restricting users from pairing Phillips Hue software with third party light bulbs, forcing users to purchase Phillips bulbs.[8]

2. Tytera M380 Modification

Tytera is a company that manufactures handheld two-way radios. A tinkerer managed to decrypt the firmware on one of their radios, the Tytera MD380.

---

[2] Copyright Office, "Section 1201 of Title 17," June 2017 ("1201 Report"), at 89.
[3] PHILIPS HUE, http://www2.meethue.com/en-us .
[4] *Custom Firmware Hue Lights*, PEEVEEONE (Nov. 16, 2016), https://peeveeone.com/?p=187.
[5] *Zigbee Light Link*, ZIGBEE ALLIANCE http://www.zigbee.org/zigbee-for-developers/applicationstandards/zigbee-light-link/ .
[6] @Hanno, TWITTER (Nov 21, 2015), https://twitter.com/hanno/status/667996639890681857.
[7] Romain Dillet, *Philips Hue DRM Blocks Third-Party Light Bulbs*, TECH CRUNCH, (Dec 15, 2015) https://techcrunch.com/2015/12/15/philips-hue-drm-update-blocks-third-party-light-bulbs/.
[8] *Id.*

Travis Goodspeed discovered a way to bypass the encryption that Tytera uses to encrypt their firmware updates.[9] According to Goodspeed, users can bypass the encryption by obtaining a previous version of the firmware from the Internet Archive and unpacking it. This produces a decrypted firmware binary image. The user must then load the new firmware and load a core dump of RAM.

The new modified firmware opens up new potentials for users. In digital mobile radio, audio is sent through either a public talk group or a private contact.[10] Custom firmware packages can allow a user to monitor private talk groups and private calls which would normally be unavailable but for the modification.[11] With the modified firmware, users may install other firmware updates, for example to reprogram side buttons or reset the backlight timer.[12]

3. TucoFlyer (Camera Gimbal Modification)

Micah Elizabeth Scott, a robotics expert that often live-streams her projects on the web, circumvented the encryption protecting a camera gimbal's application firmware to modify the original firmware. Scott's creation, dubbed the TucoFlyer, is a pulley-enabled suspended robot that utilizes this modified gimbal to track and record Tuco, Scott's cat.[13]

To decrypt the block cipher mode of operation that protected the gimbal's firmware, Scott discovered an enabled open serial wire debug port when the application was operating normally. Scott dumped the firmware's RAM, and with the help of an online video viewer, brute forced each offset in the file and decrypted the firmware blocks.

By reverse engineering the firmware, Scott was able to control the gimbal and reprogram its motors for new uses.

User modifications such as the TucoFlyer provide users with new, previously unavailable uses for their devices. In this instance, Scott wanted a device to autonomously record her cat for live-stream videos. Scott dismissed the idea of purchasing a quadcopter drone and opted for designing a device that was much safer and quieter.[14] The camera gimbal contained image tracking and 3-axis stabilized movement which enables the mounted camera to track moving subjects and smoothly record video while the device itself is moving.[15] Without solving the

---

[9] Travis Goodspeed, *Reversing MD380 Firmware with IDA Pro*, https://github.com/travisgoodspeed/md380tools/wiki/IDAPro.

[10] *Jailbreak Firmware Now Available for Cheap Digital Walkie-Talkie Allowing DMR Scanning*, (Jan. 29, 2016), http://phasenoise.livejournal.com/1142.html.

[11] *Id.*

[12] Travis Goodspeed, *Python Tools and Patched Firmware for the TYT-MD380*, https://github.com/travisgoodspeed/md380tools.

[13] *004-0x0FF the Rails*, Unnamed Reverse Engineering Podcast (Oct. 13, 2017), http://reverseengineering.libsyn.com/004-0x0ff-the-rails.

[14] Micah Elizabeth Scott, *Winch Bot – scanlime:026*, (Sept. 12, 2017), https://www.youtube.com/watch?v=s3O0jKvxUIM.

[15] FEIYU-TECH, http://www.feiyu-tech.com/index.php/Product/detail/pr_id/84.html.

gimbal's firmware encryption, her TucoFlyer robot would not have had the ability to safely and quietly track her cat.

4. AiboPet Memory Sticks Containing Modified Firmware

In 1999, Sony released Aibo (Artificial Intelligence Robot), a product line of robotic dogs.[16] An individual known by the online handles "AiboHack," and "AiboPet," (hereinafter "AiboHack") reverse engineered Aibo's firmware and produced modified firmware packages that enabled Aibo owners to teach their pets to dance, speak, obey wireless commands, and even share the video used for Aibo's vision.[17]

Although AiboHack circumvented the encryption protecting Aibo's original firmware, he did not publish his method of decryption.[18] Instead, the AiboHack website released firmware packages that users could easily copy onto a Sony Memory Stick and input into their devices.[19]

In 2001, AiboHack reportedly received a cease and desist letter from Sony, which claimed that AiboHack.com "provides the means to circumvent the copy protection protocol of Sony's Aibo Memory Stick" which constitutes "a violation of the anti-circumvention provision" of the DMCA.[20] The cease and desist letter ordered AiboHack to remove the firmware packages from the site.[21]

Sony discontinued its line of Aibo products in 2006, but the company recently announced that it will re-introduce the Aibo product line in 2018.[22] The new models will require a subscription for about $26 a month which will provide users with Wi-Fi and connectivity as well as cloud storage. AiboHack's web homepage now indicates an interest in tinkering with the re-released Sony Aibo model as well.[23]

5. Anticompetitive Use of TPMs to Control the Market for Consumables

Numerous companies that sell devices with consumable cartridges attempt to use technological restrictions to monopolize the market for replacement cartridges.

---

[16] Christopher Soghoian, *Caveat Venditor: Technologically Protected Subsidized Goods and the Customers Who Hack Them*, 6 NW. J. TECH & INTELL. PROP 46, 56 (2007).
[17] *Id.*
[18] *Id.* at 57.
[19] *Id.*; *see also* AIBOHACK.COM, http://aibohack.com/111/yart11x.htm.
[20] Carnegie Melon School of Computer Science, *Sony's Letter to "AiboPet"*, https://www.cs.cmu.edu/~dst/DMCA/AiboHack/letter2.htm.
[21] *Id.*
[22] Sam Byford, Sony Just Announced a New Aibo Robot Dog, (Oct. 31, 2017), THE VERGE, https://www.theverge.com/circuitbreaker/2017/10/31/16588878/sony-aibo-2017-announced-price-release-date.
[23] AIBOHACK.COM, http://aibohack.com/111/yart11x.htm.

Without modifying the device, a customer cannot use it with ink,[24] coffee,[25] juice,[26] cat litter box cleaning fluid,[27] or other consumables not authorized by the manufacturer.

6. PlayStation 3 Firmware Modification

The PlayStation 3 has a rich history of user modification. For example, in 2012, after a series of firmware updates by PlayStation, individuals known as "The Three Musketeers" released the "LV0 decryption key" allowing users to decrypt PS3 firmware on a PC and then re-encrypt the firmware with existing firmware keys in order to run on modified consoles.[28] The modification allows a user to run software of their choice, including installing the Linux operating system.

7. ST-Link Debugger/Programmer

The ST-Link is a device used to program standard microchips. This device itself includes encrypted firmware, which enthusiasts have modified to add new functionality.[29] The user can then archive the original firmware and replace it on the device with their preferred third-party firmware, enabling additional features.[30]

8. Repair of Hard Drives

Modern hard drives sometimes include a "self-encrypting" feature. In the case of the WD Passport external hard drive series, this encryption is flawed and insecure, yet it still interferes with the owner's ability to repair the hard drive if its controller malfunctions because data is encrypted with a key not provided to the user.[31] The result is a TPM that fails to protect access to the firmware on the hard drive or the user's files, yet locks the owner in to the manufacturer's

---

[24] Actionable Intelligence, *Is HP Up to Its Same Old Firmware Tricks?*, (Nov. 15, 2017), http://www.action-intell.com/2017/09/15/is-hp-up-to-its-same-old-firmware-tricks/.

[25] Julia Bluff, *Repairman Takes Keurig to Task over Unfixable Machines*, IFIXIT.ORG, //ifixit.org/blog/7668/unfixable-keurig/.

[26] Joel Hruska, *Investors Backing Juicero and its $400, DRM-Laden Juicer Surprised to Discover they were Fleeced*, (Apr. 20, 2017), https://www.extremetech.com/electronics/248034-investors-backing-juicero-400-drm-laden-juicer-surprised-discover-fleeced.

[27] Jorge Lopez, "The Future: A Cat Litter Box and DRM," (Dec. 21, 2014), https://jorgelo.co/the-future-a-cat-litter-and-drm-6dbda26428f8.

[28] Andy Chalk, *Hackers Release PlayStation 3 "LV0 Decryption Keys"*, THE ECAPIST, (Oct. 23, 2012) http://www.escapistmagazine.com/news/view/120288-Hackers-Release-PlayStation-3-LV0-Decryption-Keys.

[29] Lujji, *Reverse-Engineering the ST-Link Firmware*, (Oct. 13, 2016), https://lujji.github.io/blog/reverse-engineering-stlink-firmware/; Lujji, *Reverse-Engineering the ST-Link Firmware – Part 2*, (Oct. 17, 2016), https://lujji.github.io/blog/reverse-engineering-stlink-firmware-part2/.

[30] *Id.*

[31] Gunnar Alendal, Christian Kison, modg, "got HW crypto? On the (in)security of a Self-Encrypting Drive series," Sept. 28, 2015 (available at https://cyberside.net.ee/docs/1002_GotHwCryptoOnTheInSecurityOfASelf-EncryptingDriveSeries.pdf).

repair services unless they are able to circumvent. Circumvention would be necessary simply to regain access to copyrighted files the user has lawfully acquired.

9. Modification to Enable Un-Authorized Wireless Adapters in Lenovo Laptops

Lenovo machines are configured to reject wireless adapters that do not correspond to a "whitelist" of permitted devices. If a customer prefers a different adapter, the Lenovo support website has no solution other than to choose an adapter that Lenovo has authorized.[32] Users have discovered that the adapters can be made interoperable by modifying either the BIOS of the Lenovo device or the software on the adapter.[33] However, BIOS Lock technology prevents access to these software elements, requiring users to bypass BIOS Lock before using the device of their choosing.[34]

A. The Uses are Not Infringing

The Register has previously concluded that "Traditional copyright doctrines such as the idea/expression dichotomy, merger, scènes-à-faire, and fair use provide a combined and reasonable defense for many tinkering and repair activities."[35] This conclusion, and the supporting facts and caselaw, remain correct.

1. Fair Use

Fair use[36] is "a privilege in others than the owner of the copyright to use the copyrighted material in a reasonable manner without his consent."[37] Device owners who manipulate software for legitimate tinkering purposes are engaged in fair use.

a. Purpose and Character of the Use

The "central purpose" of the first factor is to determine whether or not the use in question "merely supersedes the objects of the original creation" or is transformative.[38]

Over the years, a robust body of caselaw has developed recognizing uses of copyrighted work that enable greater access to information as fair uses. Some of these cases deal specifically with analysis and modification of into functional aspects of software and have informed the Register's prior decisions to recommend exemptions for video game security research, jailbreaking, and

[32] Lenovo, *Numeric Error Code 1802 – Unauthorized network card*, https://pcsupport.lenovo.com/us/en/solutions/migr-69757.
[33] http://www.thinkwiki.org/wiki/Problem_with_unauthorized_MiniPCI_network_card.
[34] *Id.*
[35] Copyright Office, *Software-Enabled Consumer Products* ("Software Report"), at 33; *id.* at 31-41 (discussing the above in detail, as well as Section 117, as protecting numerous repair and tinkering activities).
[36] 17 U.S.C. § 107.
[37] *Harper & Row, Publrs. v. Nation Enters., Inc.*, 471 U.S. 539, 549 (1985) (internal quotations omitted).
[38] *Campbell v Acuff Rose Music, Inc.*, 510 U.S. 569, 579 (1994) (internal quotations omitted).

other software-related exemptions.

In *Sega v. Accolade*, the Ninth Circuit explained that research into the functional aspects of Sega's video game software was a legitimate purpose, even for a competitor seeking to develop competing games.[39] The court emphasized that the functional aspects of Sega's software were not copyrightable, and recognized that copying the entire software – including copyrightable elements – was necessary for analysis.[40] The court later reaffirmed this reasoning in *Sony v. Connectix*, explaining that it was legitimate for Connectix to copy Sony's Playstation BIOS in order to understand its functional parameters and allow it to create a competing means of playing games designed for the Playstation console.[41] These cases both stand for the proposition that enabling interoperability and increasing the utility of hardware are fair uses.

Just like the interoperability research of Accolade and Connectix, research involving device software for repair, modification, and diagnosis has legitimate purposes that fall well within the scope of fair use. Tinkering implicates the same software interoperability interests as those cornerstone fair use cases, and additionally implicates *hardware* interoperability, because of the embedded nature of device software. Copyright should not be a tool for manufacturers to create a monopoly in device repair parts, which is the result when users are barred from making the necessary modifications to firmware to calibrate replacement parts.

Tinkering involves a variety of transformative purposes. In the case of modification, users are literally adding new functions or modifying existing functions to suit different needs. In the case of all three categories of tinkering (diagnosis, repair, and modification), users are seeking to understand the functional aspects of the copyrighted work. The copyrightable elements of device software are incidental to such users' purpose in understanding the code's functionality. What functions exist that can be modified, or communicated with by other software and hardware? Will errors arise elsewhere if something is changed? What values must be edited to calibrate a replacement part or fine-tune performance or gas mileage? Which memory locations are available for custom software? Which memory locations correspond to variables that may be altered without circumventing an access control? What conditions cause which diagnostic codes to be issued? What will the software do when it receives a standardized command from an outside repair interface? Copyright should not prohibit device owners from answering these questions for themselves.

b. Nature of the Copyrighted Work

At least one court has found that where a portion of a software program functions as a "lockout code[]" that *must* be used to enable compatibility with independently created programs, the rightsholder's copyright interest in that portion of code is exceedingly slim. In *Static Control Components, Inc. v. Lexmark Intern., Inc.*, Static Control copied a small portion of code from Lexmark's laser printer firmware, acting on a reasonable belief that only by copying that code could Static Control build toner cartridge components that would interoperate with Lexmark

[39] *See Sega Enterprises Ltd. v. Accolade, Inc.,* 977 F.2d 1510, 1522-23 (9th Cir. 1992) (holding that using copyrighted material to study functional requirements was fair use).
[40] *Id.*
[41] *Sony Computer Entm't Inc. v. Connectix Corp.,* 203 F.3d 596, 608 (9th Cir. 2000).

printers.[42] The court held that software code used as a "lockout" bears only a thin copyright interest that is overcome by the need to use that code for interoperability.[43]

The primary nature of device firmware is functional, strongly favoring a finding of fair use. Any creative, aesthetic components are not even available for viewing when they are locked behind TPMs. *Only* by circumvention can those elements be appreciated. Since they are not ordinarily visible to customers, they are clearly not part of the market value of the work.

c. Amount and Substantiality of the Portion Used

The third fair use factor examines the amount of the copyrighted work used to determine whether the "quantity and value of the materials used are reasonable in relation to the purpose of the copying."[44] The amount taken need only be "reasonable" and for a legitimate purpose.

In *Connectix* and *Sega*, the Ninth Circuit found that copying the entirety of a software program in order to understand its functional components was necessary and therefore fair in each case. And in *HathiTrust*, *Kelly*, and *Perfect 10*, the respective courts emphasized that copying anything less than the entire work would be insufficient in order to allow enable the transformative purpose of enhancing access to knowledge.[45]

Tinkerers' access and copying of the entire firmware or an update is essential to understanding the functionality of a device[46] and determining how much storage capacity is available in the hardware for additional functionality.[47] This process requires the use of the entire work, since functionality may be found anywhere in the code and the technological process of reading the firmware off of the device or decrypting an update typically provides the entire program. Tinkerers need a full view of the firmware in order to understand how their modifications will affect its functioning. For these reasons, the use of the entire work is fair in light of the legitimate purposes of the use.

---

[42] No. CIV.A. 02-571, 2007 WL 1485770, at *5 (E.D. Ky. Apr. 18, 2007) (on remand from *Lexmark Int 'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522 (6th Cir. 2004)).

[43] *Id.* ("Regardless of whether Lexmark's [programs] were uncopyrightable lockout codes or not, SCC was reasonable in initially believing that they were.").

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

[45] *Authors Guild, Inc. v. HathiTrust,* 755 F.3d 87, 98 (2d Cir. 2014) ("For some purposes, it may be necessary to copy the entire copyrighted work, in which case Factor Three does not weigh against a finding of fair use."); *Kelly v. Arriba*, 336 F.3d 811, 820-21 (9th Cir. 2003) (holding that third fair use factor did not weigh against copier when entire-work copying was reasonably necessary); *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1165 (9th Cir. 2007).

[46] *See* Karl Koscher, et al., *Experimental Security Analysis of a Modern Automobile*, CENTER FOR AUTOMOTIVE EMBEDDED SYSTEMS 2010 IEEE Symposium on Security and Privacy 5, 9 (May 16, 2010), http://www.autosec.org/pubs/cars-oakland2010.pdf.

[47] *See, e.g.,* Tephra, Forum post to *TephraMod V7*, EVOLUTIONM.NET (Oct. 10, 2009), http://www.evolutionm.net/forums/ecuflash/451836-tephramod-v7.html (last updated Apr. 10, 2011).

d. Market for the Copyrighted Work

The fourth factor looks to direct harms to the market for the copyrighted work.[48] This factor is concerned with the harm of market substitution, not any harm caused by substantive criticism of the copyrighted work.[49] Further, "a use that has no demonstrable effect upon the potential market for, or the value of, the copyrighted work need not be prohibited in order to protect the author's incentive to create."[50]

In the case of device firmware, the copyrighted work is sold to end-users along with an entire device. The purchaser has already paid for the device, including the software, and it does not harm any copyright interest of the manufacturer for them to learn how it works and engage in lawful modification and repair.

e. Other Factors

Manufacturers have not put firmware restrictions in devices in order to protect a market for copies of the firmware. Rather, the restrictions exist to control the ways in which the hardware can be used and restrict access to information about functionality. As the Register stated in 2010, "while 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. It does not and should not infringe any of the exclusive rights of the copyright owner to run an application program on a computer over the objections of the owner of the copyright in the computer's operating system."[51]

The same analysis supports the granting of an exemption allowing device owners to tinker with the firmware that operates their devices. Whether or not manufacturers have adopted business models that benefit from restricting access to knowledge about how devices function, copyright is not a valid tool to enforce that ignorance on the public. Nor is it a valid tool to deprive users of control over their own devices and the ability to repair them.

Further, the Register has noted that Section 117 independently protects a number of repair and modification activities.[52] The passage of Section 117 also demonstrates that the purposes above are favored uses more likely to be fair.

---

[48] *Campbell*, 510 U.S. at 590.
[49] *See id*. at 591-92.
[50] *Sony Corp. of Am. v. Universal City Studios, Inc*., 464 U.S. 417, 450 (1984).
[51] Recommendation of the Register of Copyrights in RM 2008-8, Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 96-97 (June 11, 2010)), *available at* www.copyright.gov/1201/2010/initialed-registers-recommendation-june-11-2010.pdf.
[52] Software Report at 35-38.

B. The DMCA's Statutory Exemption for Reverse Engineering Is Unlikely to Apply

Section 1201(f)(1) provides a statutory exemption permitting circumvention when (1) one has lawfully obtained the right to use a copy of a computer program; (2) one acts "for the sole purpose" of identifying and analyzing elements necessary to achieve interoperability of an independently created computer program with other programs; (3) the elements of the program the user seeks to identify and analyze have not been readily available before; and (4) the acts of identification and analysis do not constitute infringement under copyright law.

Hobbyists who modify their devices' firmware to make it compatible with aftermarket parts are acting within the bounds of interoperability because they are utilizing "the ability of computer programs to exchange information and of such programs mutually to use the information which has been exchanged."[53] To the extent the software in an appliance or device needs to be repaired or modified to allow it to communicate with the software in a new part, the use would seem at first blush to fit within Section 1201(f).

However, an owner may not modify a device for the sole purpose of interoperability, but to tailor the device to best meet the owner's needs or preferences and to educate others. Many hobbyists access and modify device firmware for fun or to test and improve their own hacking skills in addition to enabling interoperability. *Reimerdes* held that such a use did not qualify for the reverse engineering exception.[54] In that case, the court found that an individual's "sole" purpose in circumventing an access control was not to ensure interoperability when that individual was part of a group that viewed circumvention "as an end in itself and a means of demonstrating [the individual's] talent."

Moreover, a hobbyist making a modification or repair to a device may well follow a set of instructions shared by other hobbyists. Such activity would fail to satisfy the requirement that the elements the hobbyist is analyzing have not been analyzed before, or might not qualify at all as "identifying and analyzing those elements of the program needed for interoperability."

The questionable applicability of Section 1201(f) is further demonstrated by the history of this rulemaking. For instance, the Librarian determined in 2010 that cell phone owners jailbreaking technological measures protecting the firmware in their phones did not "fall within the four corners" of the Section 1201(f) statutory exemption.[55] However, the Librarian's decision folded the interoperability test into a fair use analysis, finding that the use was noninfringing because it allowed firmware compatibility with specifically created applications. But ruling on an identical petition less than three years later in the 2012 rulemaking, the Librarian said that it was "unclear,

---

[53] 17 U.S.C. § 1201(f)(4).

[54] *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 320 (S.D.N.Y. 2000).

[55] Final Rule in RM 2008-8, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (July 27, 2010) ("2010 Rule") at 43829, *available at* http://www.copyright.gov/fedreg/2010/75fr43825.pdf.

at best," whether Section 1201(f) applied.[56] When even the Copyright Office is unsure whether individuals can avail themselves of the Section 1201(f) statutory exemption, class members cannot conclude with any certainty that their activities are protected. This uncertainty adversely affects lawful modification, repair, and diagnosis involving embedded software.

C. Statutory Factors

1. The Availability For Use of Copyrighted Works

Availability of copyrighted works will be improved by the proposed exemption. As described above, technical measures currently restrict the availability of device firmware for a variety of lawful uses. There will be no adverse effect on the availability of copyrighted works, since code is necessary for the devices to function and is produced for non-copyright-related reasons, and because no market harm cognizable by copyright law will result from the proposed exemption. To the contrary, additional copyrighted works will be made available that rely on the non-copyrightable information made accessible via the proposed exemption. The various videos and writings cited in this comment discussing how to repair and tinker with devices are prime examples. In the vehicle context, Craig Smith, author of the *2014 Car Hacker's Handbook*, reported that the *Handbook* was downloaded 300,000 times in the first two weeks it was available. Software patches also depend on access, including patches to fix serious vulnerabilities. Numerous tools designed to analyze and manipulate firmware also depend on the ability to access software and reverse engineer it. The availability of copyrighted works will be promoted by the proposed exemption.

2. The Availability For Use of Works for Nonprofit Archival, Preservation, and Educational Purposes

Education about engineering and tinkering will benefit from increased knowledge of device firmware to use as real-world examples in teaching and the increased ability of individuals to explore the technology for themselves. In addition, it will be possible to archive and preserve firmware on general-purpose storage media, without expensive and unreliable storage of idiosyncratic device hardware or entire appliances. Furthermore, tinkering is itself educational and is a common path for young people to become interested in studying science and engineering.[57] Copyright law should not discourage this important activity, but should permit works to be used for the educational purpose of hands-on learning.

---

[56] Final Rule in RM 20011-7, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (October 26, 2012) ("2012 Rule") at 65264, *available at* http://copyright.gov/fedreg/2012/77fr65260.pdf.

[57] *See, e.g.*, Steve Song, "In Praise of Taking Things Apart," *available at* https://manypossibilities.net/2008/03/in-praise-of-taking-things-apart/ (quoting an interview with John Seely-Brown in which he said "A huge amount of the learning that a lot of us do, that formed the foundations of all the formal education that we got afterwards, could be called 'tinkering.' Because of changes in electronics and cars, a whole generation couldn't tinker.").

3. The Impact That the Prohibition on the Circumvention of Technological Measures Applied to Copyrighted Works Has on Criticism, Comment, News Reporting, Teaching, Scholarship, or Research

As discussed above, the prohibition on circumvention curtails speech in all of the categories identified in the third statutory factor. The legal cloud resulting from the prohibition on circumvention reduces participation in research, scholarship and teaching on device functionality, repair, and modification, as well as critiquing, commenting, and reporting on the functionality of manufacturer software and potential alternatives.

4. The Effect of Circumvention of Technological Measures on the Market for or Value of Copyrighted Works

As discussed above, the relevant markets will not suffer any harm cognizable under copyright law.

5. Such Other Factors as the Librarian May Consider Appropriate

It is improper to restrict an exemption to Section 1201 on the basis of factors that form no part of the inquiry into whether the ban on circumvention has or is likely to have adverse effects on noninfringing uses of copyrighted works. Doing so contradicts the statutory language and exacerbates the constitutional flaws of Section 1201.

Section 1201(a)(1)(D) provides that an exemption shall be granted if "noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected." Thus, if the standard is met, issuing an exemption is mandatory, it "shall" issue. In making the determination of whether this standard is met, the Librarian is instructed to consider four specific factors that speak to adverse effects and infringement, and "such other factors as the Librarian considers appropriate."[58] It would be illogical to consider factors that do not bear on whether the ultimate standard is met.

Interpreting the fifth factor to grant total discretion to the Librarian also undermines the predictability and fairness of the process. Rather than relying on objective standards, a broad interpretation of factor five turns the rulemaking into an exercise in the Librarian's discretion, and invites the consideration of questions lying far beyond the Librarian's expertise and mandate. The First Amendment does not permit a speech-licensing regime with such open-ended decisionmaking powers.

D. Definition of Software-Enabled Devices

The Copyright Office previously determined that it would be difficult to define "software-enabled consumer devices" as a category.

In the first instance, this exercise is simplified by not limiting the exemption to "consumer devices."

[58] 17 U.S.C. 1201(a)(1)(C)(v).

The right to repair, diagnose, and modify devices *are* concerns general to all devices that run software. To the extent that particular categories of software or devices seem to be exceptions to that rule or to present special complications, the inquiry should be how to define a category that will be carved out from the general rule permitting such noninfringing activities.

E. Definition of Permitted Modifications

Copyright law allows for a wide range of noninfringing modifications to device software. The exemption language can lean on that breadth and flexibility by applying to "modifications that do not infringe copyright." This encompasses the wide range of legal doctrines that the Copyright Office found to be relevant to this issue, including Section 117, fair use, merger, scenes-a-faire, and the idea/expression dichotomy. It would be duplicative to attempt to re-write those fact-specific doctrines in the exemption language.

Again, the breadth of examples demonstrates that the need for modifications is a general one, and to the extent that particular forms of noninfringing modifications raise concerns, those concerns should be addressed without condemning the wide range of legitimate innovations and customizations that are enabled by user modification.