UNITED STATES COPYRIGHT OFFICE

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

Initial Comment of Matthew Green Regarding Proposed Class 10

ITEM A. COMMENTER INFORMATION

Commenter:

Matthew Green

Representative:

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

ITEM B. PROPOSED CLASS ADDRESSED

Proposed Class 10: Computer Programs—Security research

ITEM C. OVERVIEW

Security research is essential to the well-being of those who are subject to digital technology. The permanent and temporary exemptions existing for security research are unnecessarily limited and harm the public by failing to allow important, noninfringing security research. In particular, the limitation of the temporary exemption to "a device or machine that is primarily designed for use by individual consumers" fails to alleviate the adverse impact of the ban on circumvention on research into a variety of devices on Green's research agenda.

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

Dr. Green seeks to circumvent the myriad types of TPM documented in the 2015 Rulemaking inquiry into security research, such as encryption.

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

Many computer systems used today have serious vulnerabilities. Wrongdoers identify these vulnerabilities and then exploit them for their own malicious purposes—to defraud, to steal someone's identity, to stalk, or just to invade people's privacy.

Independent security researchers like Dr. Green identify those vulnerabilities so they may be fixed. To analyze the security of a given technology, Dr. Green or a member of his team will first

purchase a copy of the system they wish to test. This might be software, or a device, or a set of devices. Dr. Green then seeks to understand how the system works, and where it might be vulnerable.

A rigorous and effective audit of a computer system's security requires that Dr. Green analyze the software controlling the system. Often, secure computer systems prevent access to their software code through TPMs such as encryption, username/password combinations, or physical memory restrictions preventing a user from accessing certain stored information.

An adversary seeking to extract information about the software code or about the system's user, or to install their own malicious software, would seek to bypass these measures in order to maximize their ability to locate and exploit vulnerabilities. To identify security flaws, Dr. Green must do the same; indeed, finding and reporting on the vulnerability of these access controls is a critical part of auditing the security of the system.

If he does not bypass access controls in a computer system, Dr. Green's research is significantly limited. While he may be able to discover some vulnerabilities, he cannot determine with confidence whether devices are secure against an adversary willing to circumvent access controls. Often, they are not.

For instance, in the fall of 2015, Dr. Green chose to perform a limited analysis on one of the subjects of his research, treating it as a "black box" with certain inputs and outputs rather than looking inside to explore the code that controlled it. This approach limited his ability to understand (and fix) the system and its potential flaws.

A. The Copyrighted Works

Dr. Green's research agenda includes industrial-grade firewall and private network modules, hardware encryption devices, toll collection systems, non-implantable medical devices, and wireless communication systems that connect vehicles to one another and to the surrounding infrastructure.

If the Librarian did not intend to exclude such devices, the unnecessary limiting language "that is primarily designed for use by individual consumers" may be deleted. Simply adding a laundry list of the particular technologies identified by Dr. Green would be unnecessarily narrow; the existence of this wide range of need demonstrates that the limitation related to individual consumers is misguided.

B. The Adversely Affected Uses Are Noninfringing

The legal analysis for non-consumer devices is the same as for the other devices the Librarian has exempted. Security research is a noninfringing use and is adversely impacted by the ban on circumvention of access controls.[1]

[1] *See, e.g., Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1520 (9th Cir. 1992) (copying incidental to reverse engineering of video game program is a protected fair use); *Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596, 602-603 (9th Cir. 2000) (copying incidental to

The requested exemption is necessary to enable research and scholarship into device security and safety. This research is an archetypical fair use codified in Section 107, undertaken to enhance public knowledge about the functioning of software that affects the health and financial security of hundreds of millions of Americans.

In the course of engaging in security and safety research, an individual may copy the code (typically onto a general-purpose computer for analysis), modify the code (for example, to detect or patch a security vulnerability or safety issue), and distribute the code as part of scholarly discourse. Such discourse could include criticism of the code's flaws, positive scholarship regarding its approach to security or safety, or reporting on matters of public interest, including vulnerabilities and bugs. These acts potentially implicate the exclusive rights granted to copyright owners, but are lawful as fair uses.

1. 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.[2] Research and scholarship are purposes that are explicitly called out in Section 107 as supporting a finding of fair use.

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 research into functional aspects of software and have informed the Register's prior decisions to recommend exemptions for security research, jailbreaking, and 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.[3] The court emphasized that the functional aspects of Sega's software were not copyrightable, and recognized that copying the entire software program, including any copyrightable elements, was necessary for analysis.[4] 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.[5]

Additional cases have reaffirmed that increasing public access to information is a legitimate and important purpose that supports a finding of fair use, including book search and image search

---

reverse engineering video game operating system is a protected fair use); 2015 Rulemaking, Register's Recommendation at 303.

[2] *Campbell v. Acuff Rose Music, Inc.*, 510 U.S. 569, 579 (1994) (internal quotations omitted).

[3] *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).

[4] *Id.*

[5] 203 F.3d 569, 608. (9th Cir. 2000).

functions.[6] In light of such cases, the Copyright Office has recommended exemptions for security research on a variety of devices and machines.

Just like the functional research of *Accolade* and *Connectix*, security and safety research has a legitimate purpose that falls well within the scope of fair use.

Copyrightable elements of software are incidental to researchers' purpose in understanding and critiquing the code's functionality, which is where vulnerabilities and errors lie. Researchers examining software are interested in functional properties of the software. Are security and safety measures correctly implemented, or are there conditions in which they will fail? How does the code safeguard against electrical glitches? Is the computing environment as stable as as it needs to be when lives depend upon it? What is the scope of a vulnerability? Copyright should not prohibit device owners from answering these questions for themselves and informing the public.

It is well-recognized in the security community that security can only be reliably obtained when a system is subject to widespread testing.[7] The National Institute of Standards and Technology itself has warned that "System security should not depend on the secrecy of the implementation or its components" and recommended "open design."[8]

As computer security expert Bruce Schneier has said, "Basically, whenever an IT system is designed and used in secret – either actual secret or simply away from public scrutiny – the results are pretty awful. …'obscurity means insecurity.'"[9] He explains that "Security is a process. For software, that process is iterative. It involves defenders trying to build a secure system, attackers -- criminals, hackers, and researchers -- defeating the security, and defenders improving their system. This is how all mass-market software improves its security. It's the best system we have. And for systems that are kept out of the hands of the public, that process stalls."[10] "Before software bugs were routinely published, software companies denied their existence and wouldn't bother fixing them, believing in the security of secrecy. And because customers didn't know any better, they bought these systems, believing them to be secure. If we return to a practice of keeping software bugs secret, we'll have vulnerabilities known to a few in the security community and to much of the hacker underground."[11]

In addition, public scrutiny increases manufacturers' incentives to program devices carefully and to provide patches to fix known bugs and vulnerabilities.

---

[6] *See Perfect 10, Inc. v. Amazon.com, Inc*., 508 F.3d 1146 (9th Cir. 2007); *Kelly v. Arriba Soft Corp*., 336 F.3d 811 (9th Cir 2002), *Authors Guild, Inc. v. Google, Inc*., 954 F.Supp.2d 282 (S.D.N.Y. 2013).

[7] Bruce Schneier, *The Insecurity of Secret IT Systems*, SCHNEIER ON SECURITY (Feb. 14, 2014), https://www.schneier.com/blog/archives/2014/02/the_insecurity_2.html.

[8] Karen Scarfone et al., *Guide to Central Server Security*, http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf (last visited Feb. 4, 2015).

[9] *Schneier*, *supra* note 7.

[10] *Id*.

[11] *Schneier*, *supra* note 7.

The transformative, socially beneficial purpose of security and safety research on device software weighs heavily in favor of fair use.

2. Nature of the Copyrighted Work

The nature of device software weighs heavily in favor of fair use under the second statutory factor because it contains "unprotected aspects that cannot be examined without copying."[12] In *Sega*, the Ninth Circuit found the second factor to weigh in favor of fair use where copying for reverse engineering purposes was necessary to understand software's functional parameters – in that case, interoperability requirements.[13] The court explained that permitting the disassembly of copyrighted code is necessary to prevent copyright owners from gaining a "de facto monopoly" over non-copyrightable, functional components of copyrighted works.[14] It reiterated this concern in *Connectix*, explaining that "[i]f 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."[15]

Where TPMs are deployed, device owners cannot even look at the code to appreciate any expressive, copyrightable elements. The primary nature of device software is purely functional, strongly favoring a finding of fair use.

3. 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."[16]

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.[17]

Security research necessarily requires the use of the entire work, since vulnerabilities may be found anywhere in the code. The use of the entire work is fair in light of the legitimate purposes of security.

4. Market for the Copyrighted Work

---

[12] *CorpConnectix,* 203 F.3d at 603.
[13] 977 F.2d at 1526.
[14] *Id.*
[15] 203 F.3d at 605.
[16] *Campbell*, 510 U.S. at 586-87.
[17] *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*, 336 F.3d at 820-21 (holding that third fair use factor did not weigh against copier when entire-work copying was reasonably necessary); *Perfect 10*, 508 F.3d 1146.

The fourth factor looks to direct harms to the market for the copyrighted work.[18] This factor is concerned with the harm of market substitution, not any harm caused by substantive criticism of the copyrighted work.[19] 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."[20]

In the case of device software, the copyrighted work is sold along with the device. The software is of no use without a compatible device to run it. It does not harm any copyright interest of the manufacturer to analyze the purchased system to understand how it works and evaluate whether it is secure.

For these reasons, the Librarian should once again conclude that the security research adversely affected by the ban on circumvention consists of fair uses of the relevant works.

C. Statutory Exemptions

The Librarian has repeatedly recognized that the statutory exemptions do not adequately protect security research.[21] The evidence submitted in support of those conclusions remains valid.

D. Rulemaking Statutory Factors

1. Factors One Through Four

As the Copyright Office recognized in 2015, the factors favor an exemption for security research. The same reasoning applied there establishes that an exemption should issue to cover devices that are excluded by the current temporary exemption.

As in 2015, "an exemption could increase the availability of works based on security research, such as scholarly articles and presentations, as well as new computer programs aimed at rectifying discovered flaws."[22]

Further, "an exemption for good-faith security research is likely to increase the use of works in educational settings."[23] As in 2015, "the current prohibition plays a negative role in universities' willingness to engage in and fund security research, and may limit student involvement in academic research projects." *Id.* This is true in Dr. Green's experience as well.

A security research exemption also "will enhance criticism, comment, news reporting, teaching, scholarship and research" and "could enhance media attention to, and reporting on, software security issues." *Id.* at 310-311.

---

[18] *Campbell*, 510 U.S. at 590.
[19] *See id*. at 591-92.
[20] *Sony Corp. of Am. v. Universal City Studios, Inc*., 464 U.S. 417, 450 (1984).
[21] 2015 Rulemaking, Register's Recommendation at 307-309.
[22] *Id.* at 310.
[23] *Id.*

As for the effect on the market, the Register previously found the factor neutral or slightly in favor of an exemption because of the possibility "that knowledge of and ability to correct such flaws will in fact enhance the value of the software and products at issue." *Id.* at 311.

The evidence submitted in support of the Register's conclusions in 2015 remains valid and relevant and the factors continue to favor an exemption.

E. Factor Five: "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."[24] 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.

[24] 17 U.S.C. 1201(a)(1)(C)(v).