UNITED STATES COPYRIGHT OFFICE

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

Although we will not be providing multimedia evidence in connection with this comment, we provide in-text hyperlinks throughout the comment (represented as blue, underlined words) that link to documentary evidence and/or some cited documents.

ITEM A. COMMENTER INFORMATION

These comments are submitted on behalf of the Motion Picture Association of America, Inc. ("MPAA"), the Entertainment Software Association ("ESA"), the Recording Industry Association of America ("RIAA"), and the Association of American Publishers ("AAP"). They are collectively referred to herein as the "Joint Creators and Copyright Owners." They may be contacted through their counsel at Mitchell Silberberg & Knupp LLP, J. Matthew Williams, 202-355-7904, mxw@msk.com, 1818 N. Street, NW, 8th Floor, Washington, D.C. 20036.

The Motion Picture Association of America, Inc. ("MPAA") is a trade association representing some of the world's largest producers and distributors of motion pictures and other audiovisual entertainment material for viewing in theaters, on prerecorded media, over broadcast TV, cable and satellite services, and on the internet. The MPAA's members are: Paramount Pictures Corp., Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corp., Universal City Studios LLC, Walt Disney Studios Motion Pictures, and Warner Bros. Entertainment Inc.

The Entertainment Software Association ("ESA") is the United States trade association serving companies that publish computer and video games for video game consoles, handheld video game devices, personal computers, and the internet. It represents nearly all of the major video game publishers and major video game platform providers in the United States.

The Recording Industry Association of America ("RIAA") is the trade organization that supports and promotes the creative and financial vitality of the major music companies. Its members are the music labels that comprise the most vibrant record industry in the world. RIAA members create, manufacture and/or distribute approximately 85% of all recorded music produced in the United States.

The Association of American Publishers ("AAP") represents the leading book, journal, and education publishers in the United States on matters of law and policy, advocating for outcomes that incentivize the publication of creative expression, professional content, and learning solutions. As essential participants in local markets and the global economy, our members invest in and inspire the exchange of ideas, transforming the world we live in one word at a time.

The Joint Creators and Copyright Owners all rely on technological protection measures to offer innovative products and licensed access to consumers. Access controls make it possible (i) for consumers to enjoy recorded music through subscription services like SiriusXM, Spotify, Amazon Music Unlimited, YouTube Red, Apple Music and Pandora, including on mobile devices, through in-home voice assistants, and in their vehicles; (ii) for consumers to view motion pictures at home or on the go via discs, downloadable copies, digital rental options, cloud storage platforms, TV Everywhere, video game consoles, and subscription streaming services; (iii) for consumers to play their favorite video games on consoles, computers, and mobile devices; and (iv) for consumers to enjoy and learn from books, journals, poems and stories (including through subscription, lending, and rental options) on dedicated e-book readers, such as the Kindle and the Nook, on tablets and smartphones, and via personal computers. As the Register concluded in the recent Section 1201 Study, "[t]he dramatic growth of streaming

services like Netflix, Spotify, Hulu, and many others suggests that for both copyright owners and consumers, the offering of access—whether through subscriptions, *à la carte* purchases, or ad-supported services—has become a preferred method of delivering copyrighted content. . . . [T]he law should continue to foster the development of such models." U.S. Copyright Office, *Section 1201 of Title 17: A Report of the Register of Copyrights* 45-46 (2017) ("1201 Study").

ITEM B. PROPOSED CLASS ADDRESSED

Proposed Class 10: Security Research

ITEM C. OVERVIEW

Legitimate security research is an important practice. Many companies participate in the security testing ecosystem by cooperating with good-faith researchers. As such, the Joint Creators and Copyright Owners did not oppose continuation of the existing security testing exemption, which the Register has already recommended for renewal. The existing regulatory exemption, in addition to Congress's statutory exception for security testing codified in § 1201(j), already provide the shields from liability that legitimate researchers need to circumvent access controls to conduct security testing.

The Register carefully crafted the language in the current exemption to balance the needs of legitimate researchers with the protection of not only copyrighted works, but also of the public's well-being. The Register's prior recommendation that the "Librarian exercise a degree of caution in adopting an exemption" in this arena exemplifies the importance of containing the scope of the exemption. U.S. Copyright Office, *Section 1201 Rulemaking: Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendation of the Register of Copyrights* 317 (2015) ("2015 Rec.").

Nevertheless, the proponents of the Proposed Class 10 exemption—Center for Democracy and Technology ("CDT"), Consumers Union, Professor Matthew Green ("Green"), and Professors Ed Felten and J. Alex Halderman ("Felten and Halderman")—want to delete nearly every limitation from the exemption. They attempt to justify doing so by presenting almost exactly the same arguments that they presented three years ago and during the process resulting in publication of the June 2017 Section 1201 Study, which resulted in the Register proposing that Congress utilize the current exemption as a "starting point" for drafting any new statutory exception related to security research. 2015 Rec. at 306, 312–18; 1201 Study at 71-80. The commenters' insistence on rehashing these arguments is indicative, not of legitimate frustrations with unreasonable limitations on their work, but instead of an overly antagonistic attitude toward copyright and common-sense parameters. This attitude is well illustrated by Green's meritless lawsuit against the U.S. Government. *See* Complaint, *Green v. U.S. Department of Justice*, Case No. 1:16-cv-01492 (D.D.C. filed July 21, 2016). Such philosophical objections to the law are not a proper basis for expanding a well thought-out exemption.[1]

Nor does the statute allow the Register to recommend an exemption applicable to every category of copyrighted works, which the petitioners appear to be seeking by attempting to

[1] That the commenters' philosophy is inconsistent with the law is further displayed by their attempts to redefine what is determinative of whether a person owns a copy of a computer program. Although the Register has repeatedly discussed this issue in great detail and concluded that a variety of factors impact whether a person owns a particular copy of a piece of software, Consumers Union insist that anyone "who purchases the product is the owner of the copy of the software inside it." Consumers Union, Class 10 Long Comment at 2 (Dec. 18, 2017) ("Consumers Union 2017 Comment"); *see also* Green, Class 10 Petition at 2 (Sept. 13, 2017) ("Green 2017 Petition") (suggesting that end user license agreements are irrelevant if a person "owns the physical medium that embodies the computer program"). No matter how many times the Register revisits these issues, the commenters seek to re-litigate them without any new case law to support their extreme and unfounded position.

expand the exemption to cover all works that are accessible via software operated devices. This broad-stroke approach would be an impermissible, use-based exemption, rather than an exemption for a "particular class of copyrighted works." *See* 2015 Rec. at 99 ("A mere requirement that a use be 'noninfringing' or 'fair' does not satisfy Congress's mandate to craft 'narrow and focused' exemptions. For this reason, the Register has previously rejected broad proposed categories such as 'fair use works' or 'educational fair use works' as inappropriate.").

In sum, the proponents' comments lack sufficient justification for removal of the necessary limitations specified in the current exemption. Each of the limitations in the current exemption should be maintained.

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

The proponents seek an exemption allowing circumvention of every access control used in any way to restrict access to "computer programs of all types, and including associated literary, audiovisual, and other works." Felten and Halderman, Class 10 Petition at 2 (Sept. 13, 2017).[2] Such an ill-defined class would appear to implicate nearly every access control that exists, given that digital works are accessed in ways that invariably involve the use of a computer program.

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

1. The Current Exemption's Limitations Should Be Retained.

The current regulations exempt circumvention to access:

[2] Specifically the proponents mention the need to circumvent the following: keys, shared secrets, usernames, passwords, external authentication or tethering systems, dongles, installation media, hardware fingerprinting, license prompts or click-through dialogs, obfuscation, execute-only memory or trusted platform modules, encryption, hashes, checksums, digital signatures, runtime guards, assertion checks, watermarks, external monitoring, malware and ancillary measures. Green, Class 25 Comment at 5, 7-10 (Feb. 6, 2015); Felten and Halderman, Class 10 Long Comment at 7-9 (Dec. 18, 2017) ("Felten and Halderman 2017 Comment"); Green 2017 Petition at 3; CDT, Class 10 Long Comment at 2 (Dec. 18, 2017) ("CDT 2017 Comment").

> (i) Computer programs, where the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates solely for the purpose of good-faith security research and does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986, as amended and codified in title 18, United States Code . . . , and the device or machine is one of the following: (A) A device or machine primarily designed for use by individual consumers (including voting machines); (B) A motorized land vehicle; or (C) A medical device designed for whole or partial implantation in patients or a corresponding personal monitoring system, that is not and will not be used by patients or for patient care.
> (ii) For purposes of this exemption, "good-faith security research" means accessing a computer program solely for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability, where such activity is carried out in a controlled environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement.

37 C.F.R. § 201.40(b)(7).

The petitioners focus on what they refer to as five "limitations" in the exemption that they seek to discard: the "device limitation;" the "controlled environment limitation;" the "other laws limitation;" the "access limitation;" and the "use limitation."[3] As discussed below, these "limitations" are common-sense ways of tailoring the exemption to attempt to cover only legitimate conduct. They should all be retained.

(a) The "Device Limitation"

The current exemption contains necessary limitations on the kinds of devices or machines on which access controls may be circumvented. However, one of the categories of devices that is covered is extremely broad: devices "primarily designed for use by individual consumers

[3] The petitioners appear to use the word "limitation" in a pejorative fashion. However, every exemption should contain proper limitations. That was Congress' directive to the Register and the Librarian.

(including voting machines)."[4] Whereas the Joint Creators and Copyright Owners believe that this category is overbroad and sweeps in many devices devoted to enjoying entertainment products in a manner that could already put copyright owners at risk, the petitioners claim the language is unduly restrictive. Specifically, they claim that they are unable to discern what the phrase "primarily designed for use by individual consumers" means and whether it covers "any device that a consumer indirectly uses or is a part of a larger system that a consumer interacts with." Felten and Halderman 2017 Comment at 19.

Interpreting the language to cover such devices and systems or broadening the exemption in this manner would put at risk every corporate database through which consumers obtain online information or acquire content. In 2015, the Register expressly excluded access to databases, and thus, a reading of the exemption that would include access to databases would be contrary to the Register's intent. 2015 Rec. at 252.

(b) The "Controlled Environment Limitation"

The commenters' opposition to the requirement in the current exemption that research be conducted in "a controlled environment designed to avoid any harm to individuals or the public" is particularly baseless. They complain that this language is too ambiguous. However, this claim appears to generate from a subjective desire to struggle with the language of the regulations, rather than from an objective lack of regulatory clarity.[5]

[4] The exemption also covers research on motorized land vehicles, or medical devices designed for whole or partial implantation in patients or a corresponding personal monitoring system that is not and will not be used by patients or for patient care.

[5] For example, the commenters complain that it is impossible to bring certain devices into the controlled environment of a laboratory. Felten and Halderman 2017 Comment at 39. However, the exemption does not specify that the controlled environment must be in a laboratory. It simply states that the overall testing must be controlled and "designed to avoid any harm to individuals or the public." Objecting to having to even attempt to design experiments to avoid public harm is indefensible.

Some commenters also insist that their research must be conducted in "real-life environments." Felten and Halderman 2017 Comment at 5. They posit that researchers need to work within both controlled and uncontrolled environments to protect individuals and the public. *Id.* at 23. However, as the Register concluded in 2015, opening up the exemption to include "real-life environments" would potentially harm the very individuals the researchers claim they seek to protect. Indeed, even researchers participating in support of an exemption in the sixth triennial proceeding conceded that testing live systems is dangerous. 2015 Rec. at 318. And in this current proceeding, Consumers Union supports retaining this limitation (and urges caution on abandoning the others). Consumers Union 2017 Comment at 3.

Commenters nevertheless claim they want to be free "from the burden of controlling every variable in scientific experimentation." Felten and Halderman 2017 Comment at 22. Quite simply, the exemption nowhere says that they bear such a burden. The "controlled environment" language simply requires responsible research practices. Indeed, Congress endorsed providing guidance to help define what constitutes good faith research. *See* H.R. Rep. No. 105-551, pt. 2, 105th Cong., 2d Sess., at 44 (July 22, 1998) ("The Committee recognizes that courts may be unfamiliar with encryption research and technology, and may have difficulty distinguishing between a legitimate encryption research[er] and a so-called 'hacker' who seeks to cloak his activities with this defense. Section 102(g)(3) therefore contains a non-exhaustive list of factors a court shall consider in determining whether a person properly qualifies for the encryption research defense.").

(c) The "Other Laws" Limitation

First, the petitioners suggest that the Register should recommend removal of the requirement that the device researched be "lawfully acquired."[6] However, they provide no real evidence on how their research suffers from needing to ensure the lawful acquisition of devices. CDT simply asserts that this limitation on the exemption is an "overextension of copyright law." CDT, Class 10 Petition at 3 (Sept. 13, 2017). The Register should not alter the current exemption because it aligns with the common sense approach that Congress itself adopted in the Copyright Act. *See* H.R. Rep. No. 105-796, 105th Cong. 2d Sess., at 67 (Oct. 8, 1998) ("[T]he scope of permissible security testing under the Act should be the same as permissible testing of a simple door lock: a prospective buyer may test the lock at the store with the store's consent, or may purchase the lock and test it at home in any manner that he or she sees fit. . . . What that person may not do, however, is test the lock once it has been installed on someone else's door, without the consent of the person whose property is protected by the lock.").

[6] Green's petition initially suggested the exemption should focus, not on ownership of a device, but on whether the copy of the software accessed is owned by the researcher or by a person who gives the researcher permission. However, he then proffered a flawed definition of "owner" that is contrary to the statute, the case law, and the Register's prior interpretations of the case law. Consumers' Union, in its comments, endorses a similarly flawed view of ownership. Under § 117, the fact that a person owns a device is not dispositive of whether the consumer owns a copy of a computer program resident on the device. *Vernor v. Autodesk, Inc.*, 621 F.3d 1102, 1110-11 (9th Cir. 2010) (In the Ninth Circuit, to determine whether a software user is a licensee or an owner, one must look to whether the copyright owner: (1) specified that a user is granted a license, (2) significantly restricts the user's ability to transfer the software, and (3) imposes notable use restrictions on the use of the work). The Register's prior conclusion that security testing is likely a fair use, even if not covered by 17 U.S.C. § 117 in every instance, avoided making the determination of who owns a copy of a program dispositive of whether a security-related exemption could be granted. 2015 Rec. at 300–03. While the Joint Creators and Copyright Owners do not endorse the Register's fair use analysis in every respect, this solution is preferable to adopting the misleading and legally inaccurate definition of "owner" proposed in the Green Petition, which would expressly render the language of end user licensing agreements irrelevant to the ownership analysis.

Second, the petitioners suggest that the Register should discard the requirement that circumvention must "not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986." In the Section 1201 Study, the Register recently stated that "it was not clear . . . that the requirement to comply with other laws impedes legitimate security research[, as] other laws still apply even if the activity is permitted under section 1201." 1201 Study at 80. She accordingly did not recommend any legislative reform on this point. This approach to resolving this issue remains valid based on the record in this proceeding.

The commenters claim that this language somehow "potentially exports the DMCA's harsh criminal and civil liability into other non-copyright legal regimes." Felten and Halderman 2017 Comment at 5. This is a red herring. Congress wrote a similar requirement that researchers must comply with laws other than Copyright Act into the statutory security testing exemption, § 1201(j). Thus, Congress clearly had no problem with other laws being considered in connection with § 1201. Neither should the Register. Moreover, under 17 U.S.C. § 1204(a), the research would have to be willfully in violation of § 1201 and for the purpose of commercial advantage or private financial gain to trigger criminal liability. Also, educational institutions are exempt from criminal liability under 17 U.S.C. § 1204(b). Thus, § 1201 already has built in boundaries that speak to the commenters' concerns.

(d) The "Access" And "Use" Limitations

The exemption rightfully narrows its scope to ensure circumvention is accomplished "solely" for the purpose of accessing software to conduct good faith testing, investigation, and correction of flaws or vulnerabilities. This was based on language used by Congress in multiple instances in § 1201. Oddly, Felten and Halderman seem to believe that this renders the use of the language problematic. Felten and Halderman 2017 Comment at 24. However, there is

nothing wrong with the Register attempting to ensure that security research cannot become a back door to enable unauthorized access to works and other harmful acts. In fact, that is the very task assigned to her by Congress.

The exemption also rightfully requires that the research be (i) "primarily to promote the security or safety of the class of devices or machines" at issue and (ii) that it not facilitate copyright infringement. CDT's claim that this language unfairly renders researchers responsible "for what another party does with the information" is misguided. CDT 2017 Comment at 5. The researchers are not responsible for what others do. The exemption simply holds researchers responsible for handling *their own* results with care to prevent others from misusing them to the extent feasible.

Felten and Halderman claim (again) that the language is too ambiguous, thereby limiting their speech. However, they also endorse "coordinated disclosure guidelines," stating that they "help to reduce the risk of market impacts by allowing companies time to address vulnerabilities before they are made public." Felten and Halderman 2017 Comment at 29. If the commenters desire more clearly defined rules on what may be done with the results of the research, then the Register should consider including express guidelines in the exemption regarding how the results are disseminated. For example, notifying the distributor of the software and/or device at issue of the flaw and providing reasonable time to correct the issue before publishing the results is a reasonable and preferable practice. Although the Register previously concluded that "determining the relevant 'developer' to whom information must be disclosed could be difficult, if not impossible, in some instances," 2015 Rec. at 309, that potentiality should not prevent the Register from requiring that researchers at least attempt to identify the developer, distributor, or publisher and provide an opportunity for flaw correction.

2. The Exemption Should Not Be Expanded To Cover Access To Works Beyond Computer Programs.

The commenters want to expand the exemption to allow circumvention to access *all categories of copyrightable works* for the purpose of security testing. They specifically reference "rootkit-level protection on CDs or related sound recording media, or cryptographic protections on eBooks, software manuals, DVDs, or other media accessed via software-controlled devices." Felten and Halderman 2017 Comment at 9. They refer to every type of work other than software as "ancillary works." *Id.* Their proposal is not for a "particular class of copyrighted works," as required by the statute, 17 U.S.C. § 1201(a)(1)(C), but rather is a request for an exemption based only on the type of *conduct* at issue for *all* works.

When Congress enacted § 1201, it made clear that the phrase "'particular class of copyrighted works' [is intended to] be a narrow and focused subset of the broad categories of works . . . identified in section 102 of the Copyright Act." H.R. Rep. No. 105-551, pt. 2, at 38 (1998). Based on this directive, the Register has developed an approach to crafting classes of works to be defined, initially, by reference to a sub-set of a § 102 category of works (*i.e.*, literary works in the form of computer programs), with additional limitations based on particular types of conduct (*i.e.*, security testing) and categories of users (*i.e.*, good-faith researchers). 2015 Rec. at 17-18. The commenters' proposal does not follow this framework. Instead, the proposal essentially starts, and stops, with whether a person is engaged in "security research."

Past security-testing exemptions that allowed access to works other than computer programs were based on documented security flaws applicable in specific sectors. *See* U.S. Copyright Office, *Section 1201 Rulemaking: Third Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendation of the Register of Copyrights*

53-64 (2006); U.S. Copyright Office, *Section 1201 Rulemaking: Fourth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendation of the Register of Copyrights* 174-206 (2010). The commenters have not identified any such issues that would justify enabling access to other categories of works.

Lastly, expanding the class beyond computer programs would alter the fair use analysis and the analysis of the statutory factors contained in § 1201, including the potential impact on the value of works. 17 U.S.C. §§ 107, 1201(a)(1)(C). For example, when assessing the existing exemption, the Register previously focused on the functional nature of computer software under the second fair use factor. 2015 Rec. at 301. However, including works that fall outside of the computer program category would open the door for unauthorized access, copying, and adaptation of works that would not qualify as functional, potentially exposing entertainment products and literary works to infringement. Circulating "research" regarding how to obtain unauthorized access to motion pictures, video games, books, journals, or music could cause significant economic losses. The existing exemption should not be expanded.

DOCUMENTARY EVIDENCE

The Joint Creators and Copyright Owners are not submitting any exhibits for this proposed class of works.

DATE: February 12, 2018

/s/ J. Matthew Williams
J. Matthew Williams
Dima S. Budron
Mitchell Silberberg & Knupp LLP (MSK)
1818 N Street, N.W., 8th Floor
Washington, D.C. 20036
mxw@msk.com
202-355-7904