Long Comment Regarding a Proposed Exemption

Under 17 U.S.C. 1201

Item 1. Commenter Information

Christopher Mohr, Vice President for Intellectual Property and General Counsel, Software and Information Industry Association, 1090 Vermont Avenue, Washington D.C.

Item 2. Proposed Class Addressed

Class 10: Security

Item 3. Overview

SIIA is the principal trade association of the software and information industries and represents over 800 companies that develop and market software and digital content for business, education, consumers, the Internet, and entertainment. SIIA's members range from start-up firms to some of the largest and most recognizable corporations in the world, and one of SIIA's primary missions is to protect their intellectual property and advocate a legal and regulatory environment that benefits the software and digital content industries. SIIA member companies are market leaders in many areas, including but by no means limited to:

- software publishing, graphics, and photo editing tools
- corporate database and data processing software
- financial trading and investing services, news, and commodities exchanges
- online legal information and legal research tools
- protection against software viruses and other malware and
- education software and online education services

Our members depend on section 1201 to protect their works from infringement, and SIIA has participated in every rulemaking since the statute's enactment.   In our view, Section 1201 has succeeded in performing its intended purpose: namely, to accomplish the "mutually supportive" goals of a "thriving electronic marketplace [that] provides new and powerful ways for the creators of intellectual property to make their works available to legitimate consumers in the digital environment," and a plentiful supply of intellectual property" to drive the demand for a more flexible and efficient marketplace."[1] Congress properly recognized that "the digital environment poses a unique threat to copyright owners" and that it "necessitates protection against devices that undermine copyright interests."[2]

As a group, the supporters of an expanded exemption want several limitations removed from the security research exemption: as they describe them, the "Device Limitation," the "Other Laws" limitation; the "Controlled Environment Limitation"; the "Access Limitation", and the "Use Limitation."[3] Put in the affirmative, petitioners would like to be able to circumvent TPMs on a computer program for good-faith security research:

- no matter what kind of device the computer program runs on—industrial, or a cloud server;
- even if the security research served another commercial and directly competitive purpose beyond advancing the state of the security research field;
- no matter the environment in which the security testing occurs and the threat of harm to the public or copyright owners;
- even if the act of security research violates any number of laws, including the Consumer Fraud and Abuse Act (18 U.S.C. 1030);
- irrespective of whether the result of the circumvention is primarily used in a manner that facilitates copyright infringement and is primarily used to destroy the security or safety of either the users of the system or the system itself.[4]

While we did not support the reissuance of the security exemption promulgated during the 2015 Rulemaking, SIIA intentionally did not oppose its reissuance due to the fact that it was cabined with a number of reasonable conditions and limitations. Petitioners seek to remove those limitations. SIIA therefore opposes the proposed expansion as legally impermissible and unsupported by record evidence.

[1] H. Rep. 105-551 (Part II), at 23.

[2] *Id.* at 25.

[3] Felten Comment, at 2.

[4] *See id.*

Remaining Items.

SIIA objects to petitioners' proposed class as overbroad. The Register has stated that

> "the description of the "particular class" ordinarily will be refined with reference to other factors so that the scope of the class is proportionate to the scope of harm to noninfringing uses. For example, a class might be refined in part by reference to the medium on which the works are distributed, or to the access control measures applied to the works. The description of a class of works may also be refined, in appropriate cases, by reference to the type of user who may take advantage of the exemption or the type of use that may be made pursuant to the designation. The class must be properly tailored to address not only the demonstrated harm, but also to limit the adverse consequences that may result from the exemption to the prohibition on circumvention. In every case, the contours of a class will depend on the factual record established in the rulemaking proceeding."[5]

By deleting the restrictions that make the security testing exemption narrow, what petitioners have done is to create a security testing exemption that applies to all computer programs, regardless of the access controls used, or the medium in which the works are distributed. While the Office has acknowledged that a class of user may help define a class of work, it must do so in conjunction with other factors that narrow the class. Such an exemption lies beyond the scope of the Register's statutory authority.

Second, petitioners' link between their proposed exemption and non-infringing use of computer programs is not as clear as they would have it seem. Petitioners state that the "functional elements, such as a computer program's object code, which contains ideas and execute tasks, are excluded from copyright protection."[6]

While it is true that, as *Connectix* stated, the BIOS at issue in the case had to be copied to be analyzed for purposes of reverse engineering for interoperability purposes,[7] that decision said so while analyzing fair use. One cannot, from these cases, infer that computer programs receive any more (or less) protection than any other kind of literary work. In *Connectix,* one of the reasons for permitting the copying of the computer program was because the BIOS software did not project a screen display that revealed its functioning, and that information

[5] 75 Fed. Reg. at 65260, 65261 (October 26, 2012). *See also*

[6] Felten Comment, at 11 (citing *Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596, 602 (9th Cir. 2000) (citing 17 U.S.C. § 102(b)).

[7] *Connectix*, 203 F.3d at 603.

about it was not publicly available.[8] Similarly, if use of the software exceeds the scope of a license, infringement will generally lie.

Petitioners neither acknowledge nor propose any of these limitations. Their proposed limitations should be rejected.

The Evidence for a Broad Exemption is Lacking.

As an initial matter, SIIA questions any suggestion that cybersecurity research in general is suffering from the absence of a broader exemption. Adverse effects on that industry seem missing, as investment and revenues are growing at a rapid rate and have doubled several times in years when the Office did not issue an exemption.[9] At the same time, SIIA also did not oppose re-issuance of the 2015 exemption because it believed that exemption to be sufficiently cabined and

Petitioners have requested that the Copyright Office throw those sensible limitations by the wayside. The evidence of adverse effects cited by petitioners is insufficient to support the breadth of the exemption that they request.

Other Laws, Controlled Environment, Access, and Use

It is SIIA's position that if another statute prohibits the act of circumvention, then an exemption cannot issue. As interpreted by the Register, section 1201 must be "*the* cause" of the adverse effects that allegedly support the petition.[10] Here, the existing exemption for security research requires that the user's activity not be in violation of other statutes, most notably the CFAA. This limitation ensures that section 1201 is the factual and legal cause of any adverse effects that may exist. Conversely, if the CFAA (or a similar statute) prevents certain activity, then 1201 does not cause the adverse effect as a matter of law.

Legal reasoning aside, the "other laws" limitation should remain. The idea that a private citizen should be permitted by the DMCA to hack into a flying aircraft or a building's climate control system is not terribly comforting.[11] More to the point, many copyrighted works are made available on platforms or over networks. It is for this reason that SIIA views the

[8] *Id.* at 604.

[9] Gartner Says Worldwide Information Security Spending Will Grow 7 Percent to Reach 84.7 Billion in 2017, https://www.gartner.com/newsroom/id/3784965; Cybersecurity market report, https://cybersecurityventures.com/cybersecurity-market-report/ (noting that security market has increased thirty-five fold in the last thirteen years, and is predicted to have

[10] 1201 Study, at 115 (emphasis supplied).

[11] *See* Felten Comment, at 22-23.

"device limitation" and the "other laws" limitation as a sensible protection against piratical anti-circumvention activity.

Should the Office be tempted to eliminate the so-called "device limitation," SIIA urges circumspection. We acknowledge that making truly "harmless" connection attempts to *publicly available* computers is not an activity that SIIA or its members would necessarily object to. The difference (to use an admittedly simplified analogy) is difference between walking through a neighborhood at night and seeing who left their blinds up, picking the front door lock, or looking through the window in a way that turns the passerby into a tortfeasor. The difference between these fact patterns is usually set through shared set of customs and usages generally followed by the security community and those who they seek to protect.[12]

As to the "use" limitation, petitioners seek to expand the scope of the anti-circumvention provision beyond the text of the statute.[13] They argue that the use limitations chill their ability to publish research.[14] Case law has settled the difference between the source code for a particular circumvention tool, discussion of the tool, and use of the tool itself.[15] We are aware of no case that would prevent petitioners from being able to "inform consumers that the system is insecure so they can protect themselves."[16]

The reason for that expansion stems from the allegation that the word "primarily designed for" could be a subjective test or an objective test.[17] We agree with the petitioners that the words require intent on the part of the security researcher.[18] That intent can be proven through statements of subjective intent followed by objective indicia showing that the designers' words matched their action. Resolution of such factual questions is neither new to

[12] *Cf. id.* at 37 ("norms and customs of academic research require that we only attempt to exploit vulnerabilities in these systems with the prior permission of the owner—though not the holder of copyright in the software in the system—and we conduct any investigation into such systems in ways that would not cause risk or harm to any person."). SIIA notes that it is exactly this practice which is codified in the text of the exemption itself. 17 U.S.C. § 1201(j)(1). The DMCA does not prevent accessing a computer so long as permission exists.

[13] *See id.* at 24.

[14] *See id.* at 39-40.

[15] *E.g.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429, 445–46 (2d Cir. 2001).

[16] Felten Comment, at 40.

[17] *See* Felten Comment. at 18.

[18] *See id.* at 39-40.

the law generally or copyright in particular. We believe that the language permits—as it should—flexibility to identify bad actors on a case by case basis.

With that said, SIIA has no bone to pick with good-faith security research. Although we may disagree with several parts of their arguments and oppose their suggested revisions to the existing regulation, we do not believe that petitioners are interested in committing, facilitating or enabling copyright infringement. SIIA is, instead, concerned that others will misuse an overbroad exemption to place works in the clear, and by so doing cause harm to copyright owners.