July 12, 2018

Steven R. Englund
Tel 202-639-6006
senglund@jenner.com

Regan A. Smith
General Counsel and
Associate Register of Copyrights
United States Copyright Office
Library of Congress
101 Independence Avenue SE
Washington, DC 20559-6000

Re: Section 1201 Rulemaking (Docket No. 2017-10): Election System Providers' Response to letter from CCIPS with respect to Proposed Class 10

Dear Ms. Smith:

Thank you for your letter dated June 29, 2018, providing participants in the Copyright Office's Section 1201 rulemaking proceeding with the opportunity to respond to the letter dated June 28, 2018 that you received from the Computer Crime and Intellectual Property Section of the U.S. Department of Justice's Criminal Division ("CCIPS"). Dominion Voting Systems, Election Systems & Software, and Hart InterCivic (collectively, the "Election System Providers") respectfully submit that the CCIPS letter largely echoes the comments provided by other proponents of proposed Class 10, and does not provide meaningful support for the Register's recommending Class 10 as an exemption.

The Election System Providers agree with CCIPS that computer security is important. That is why the Election System Providers design their hardware and software to secure such products against threats presented in the environments in which they are used, and offer products that have been certified by the U.S. Election Assistance Commission after independent testing to ensure that they meet high standards of functionality, accessibility and security.

Although the Election System Providers respect and appreciate CCIPS' important work preventing, investigating, and prosecuting computer and intellectual property crimes, CCIPS' approach to this proceeding is backward. Its basic premise is that because good faith security research is important, limitations on the existing security research exemption should be eliminated to promote such research. *See generally* CCIPS Letter at 2-5. However, current U.S. law with respect to circumvention is that circumvention is prohibited unless a statutory exemption applies or the Librarian determines that an exemption should be granted based on a specific statutory standard. *See* 17 U.S.C. § 1201(a). The limitations on the existing security research exemption are ones the Register found necessary in 2015 based on application of the standard in Section 1201(a)(1)(C) to the record of that proceeding. 2015

Register's Recommendation at 316-19. The CCIPS letter does not make any effort to argue that the record in this proceeding is materially different or that the standard in Section 1201(a)(1)(C) would be satisfied with the elimination of what CCIPS and the other proponents have referred to as the device limitation and the controlled environment limitation.[1] Because the Office's role in this proceeding is to apply the law as it exists, and particularly the standard in Section 1201(a)(1)(C), the CCIPS letter is of little relevance to the task at hand.

Concerning the specific points addressed in the letter, CCIPS asserts that the phrase "good-faith" is so meaningful a limitation on the security research exemption that the Register could dispense with other limitations she found important in 2015. CCIPS Letter at 3. This approach puts too much weight on the concept of good faith. Good faith is a subjective standard. *E.g., Rossi v. Motion Picture Ass'n of America Inc*., 391 F.3d 1000, 1004 (9th Cir. 2004) (citing cases). By contrast, the Register is charged with recommending "particular class[es] of works" that should be exempt from Section 1201(a)(1)(A). 17 U.S.C. § 1201(a)(1)(C). While the Register may "in appropriate circumstances" define such a class in part "by reference to the particular type of use and/or user to which the exemption will apply," 2015 Register's Recommendation at 18, it would be inappropriate to define a "class of works" significantly based on a particular circumventing party's subjective beliefs about what constitutes proper "testing, investigation and/or correction of a security flaw or vulnerability." 37 C.F.R. 201.40(b)(7)(ii). Relying on the concept of good faith to the extent advocated by CCIPS would certainly represent a major departure from the Register's past approach of recommending exemptions for classes of works that are narrowly-tailored and well-defined.

The CCIPS letter also does not provide a proper basis for the Register to recommend elimination of the device limitation and the controlled environment limitation. The Register recommended the device limitation in 2015 because she found that the "record [did] not support the open-ended exemption urged by [the] proponents, encompassing all computer programs on all systems and devices." 2015 Register's Recommendation at 317. Accordingly, she found that the "exemption should encompass the types of software that were the focus of the record in [the] proceeding." *Id*. The record in this proceeding is not meaningfully different, in that the proponents of Class 10 have provided a wish list of types of software as to which they might be interested in carrying out research, but made no particularized effort to apply the standard in Section 1201(a)(1)(C) to the unique characteristics of the various types of software. As in 2015, "[n]o showing was made to justify access to other types of software or systems or explain how such an exemption would work." *Id*. The CCIPS letter does not address this gap in the record, and instead assumes that exemption should be the norm, with the burden being on the opponents or the Register to supply a "rationale ... for limiting the security research exemption." CCIPS Letter at 4.

---

[1] The CCIPS letter discusses what the proponents have referred to as the other laws limitation, but CCIPS does not advocate eliminating the requirements that research (1) be conducted with a lawfully acquired copy of the relevant software and (2) not violate other law, or at least the Computer Fraud and Abuse Act. CCIPS Letter at 5-6.

As to election systems, it is clear from the record that they are situated differently from software embedded in products that are readily accessible to individual members of the public. Voting machines are accessible to individuals only under tightly controlled conditions, and access to other election systems is even more tightly controlled. Election System Providers Comments at 3, 6-8. Neither CCIPS nor the other proponents has meaningfully addressed the implications of such controlled access for analysis of whether their proposed use case is noninfringing or significantly limited by Section 1201. *See* Election System Providers Comments at 9-10, 16-20.

The CCIPS letter also accepts the other proponents' false dichotomy between research "conducted in realistic conditions," CCIPS Letter at 5, and research "carried out in a controlled environment designed to avoid any harm to individuals and the public," 37 C.F.R. § 201.40(b)(7)(ii). The existing regulatory language plainly does not require that permissible research be carried out in unrealistic conditions; it requires that researchers control the environment to avoid harm. CCIPS is right when it states that "reducing the risk of harm to the public is critically important." CCIPS Letter at 5. In view of that, it would be irresponsible to eliminate the controlled environment limitation based on fears that are not supported by the actual regulatory language.

CCIPS ultimately seems to support retention of the requirement that circumvention occur using a copy of the software that has been lawfully acquired. CCIPS Letter at 5. However, its discussion of that requirement obscures the critical point that much election software – like much other software that is not embedded in devices – is licensed only to particular users and only under agreed-upon terms. A state or local government that has lawfully acquired election software for its own use conducting elections in its jurisdiction could not reproduce and distribute a copy of that software to an independent researcher without infringing. *See* 17 U.S.C. § 106(1), (3); Election System Providers Comments at 17-20.

Notably, while the CCIPS letter recites the Department of Justice's "number of distinct interests with respect to the DMCA," CCIPS Letter at 2, the letter does not purport to speak on behalf of the Department as a whole, much less the Administration as a whole.[2] Instead, the letter expresses a policy view of CCIPS alone.

CCIPS' expressing its policy view at this time is highly irregular. Earlier in this proceeding, the Office prescribed an orderly approach to comments in this proceeding, with proponents being required to make their cases last December and opposition comments due in February. Reply comments were permitted in March, but the Office instructed that they "should not raise new issues" and "instead be limited to addressing arguments and evidence presented by others." Notice of Proposed Rulemaking, 82 Fed. Reg. 49,550, 49,558 (Oct. 26, 2017). CCIPS' comment is not a proper reply comment under the rules of this proceeding, so it is more than six months too late. While the Election System Providers appreciate

[2] In 2015, "views within the Administration ... appear[ed] to be sharply divided on the issues surrounding security research and the wisdom of granting an exemption for this purpose." 2015 Register's Recommendation at 316.

the opportunity to comment yet again in response, the Office's acceptance of multiple rounds of late comments from proponents is nonetheless unfair, because the opponents of the proposed exemption have been forced to engage in an expensive, disruptive and disjointed process of responding piecemeal to the proponents' arguments, rather than being able to understand the proponents' complete case and provide a comprehensive response as contemplated by the Notice of Proposed Rulemaking.[3] No further late comments should be accepted and the Office should stand by the timeframes it has outlined previously.

For the foregoing reasons and those stated in our comments, the Office should attach no weight to the CCIPS letter and decline to recommend the proposed exemption as to election systems.

Sincerely,

/s/ Steven R. Englund
Steven R. Englund
JENNER & BLOCK LLP

Counsel for the Election System Providers

[3] The Office's acceptance of multiple late comments also seems likely to encourage further disregard of the Office's procedures in the future.