July 13, 2018

via email

Regan A. Smith
General Counsel and Associate Register of Copyrights

Kevin Amer
Senior Counsel for Policy and International Affairs

United States Copyright Office, Library of Congress

Re: Docket No. 2017-10
2017–2018 DMCA Section 1201 Triennial Review
Proposed Class 10—Security Research
Letter from Department of Justice Computer Crime and Intellectual Property Section

Dear Ms. Smith and Mr. Amer,

On behalf of Prof. J. Alex Halderman and the Center for Democracy and Technology, thank you for your continued consideration of Proposed Class 10 in the above-referenced proceeding, aimed at addressing key limitations and ambiguities in the existing exemption to the anticircumvention measures in Section 1201 of the Digital Millennium Copyright Act (DMCA) that chill good-faith security research. We appreciate the opportunity to comment on the June 28 submission of the Computer Crime and Intellectual Property Section (CCIPS) of the Department of Justice's Criminal Division[1]

Accepting the CCIPS Letter into the Record. At the outset, we support the Office's decision to accept the CCIPS letter into the record and solicit additional notwithstanding its submission after the written comment period.[2] The consideration of substantial relevant evidence is consonant with the Office's obligation in Section 1201(a)(1)(C) to conduct the triennial review as an open-ended rulemaking proceeding subject to the provisions of the Administrative Procedure Act,[3] which requires "giv[ing] interested persons an opportunity to participate in the rule making through submission of written data, views, or arguments,"[4] and not as an adversarial

---

[1] https://www.copyright.gov/1201/2018/USCO-letters/USDOJ_Letter_to_USCO.pdf; *see also* Letter from Regan Smith to Class 10 Hearing Participants (June 29, 2018) (on file with counsel).

[2] Smith Letter

[3] 17 U.S.C. § 1201(a)(1)(C).

[4] 5 U.S.C. § 553(c).

litigation matter where probative evidence is barred by unforgiving procedural hurdles. Moreover, CCIPS' perspective on the ambiguities and limitations at issue in the presumptively renewed security research exemption is particularly relevant to understanding the chilling effects of potential criminal liability for non-infringing activities because CCIPS is directly responsible for prosecuting criminal violations of Section 1201.

The Important Role of Independent Security Research. We acknowledge, agree with, and appreciate CCIPS' description of the important role that independent security researchers play in serving the critical public interest of cybersecurity, including "identifying errors and vulnerabilities in software, digital devices and networks, developing solutions to fix them, and preventing them from being exploited by criminals."[5] We likewise agree with CCIPS that many opponents to the exemption have sought to narrow the proposed exemption for reasons unrelated to the DMCA's ultimate purpose of "protect[ing] exclusive rights protected by copyright" and that, contrary to opponents' contentions, the DMCA is "not the sole nor even the primary" legal basis for "defining the contours of appropriate [security] research."[6] We also agree with CCIPS' observation that the scope of the security researchers' behavior is substantially governed by laws other than Section 1201 as well as professional norms and academic guidelines.[7]

The Good-Faith Limitation in the Existing Exemption. Moreover, we agree with CCIPS that the inclusion of the limiting phrase "good faith" in the existing security research exemption[8] meaningfully limits the ability for bad actors to abuse the exemption's applicability to scenarios that clearly do not fall within the ambit of legitimate research, such as exploiting security vulnerabilities in software for the purpose of willful copyright infringement, extortion, or illicit financial gain.[9] This understanding of the phrase obviates the need to include the bewildering array of vague limitations that we have proposed removing from the next iteration of the exemption.

---

[5] *See* CCIPS Letter at 2.

[6] *See id.* at 3

[7] *See id.*

[8] 37 C.F.R. § 201.40(b)(7).

[9] *See CCIPS Letter* at 3.

The Device Limitation. Our comments urged removing the Device Limitation from the existing exemption[10] on two basic grounds: it has an ambiguous scope that generates uncertainty among researchers about eligibility for the exemption and is unjustifiable as good cybersecurity policy.[11] CCIPS confirms each of these points explicitly in its support for eliminating the Device Limitation.[12]

First, CCIPS notes its view that the "primarily designed for use by individual consumers" language is "amenable to different interpretations and may not provide the degree of certainty necessary for prospective security researchers to be reasonably sure that their activities will be exempted."[13] CCIPS also emphasizes that "it appears there is little agreement [among commenters] as to what the phrase

---

[10] *See* 37 C.F.R. § 201.40(b)(7)(i)(A)-(C) (". . . 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.").

[11] Comments of Prof. Ed Felten and Prof. J. Alex Halderman at 5, 18-21, https://www.copyright.gov/1201/2018/comments-121817/class10/class-10-initialcomments-felten-halderman.pdf; Comments of CDT at 2-4, https://www.copyright.gov/1201/2018/comments-121817/class10/class-10-initialcomments-cdt.pdf; Reply Comments of Prof. Ed Felten, Prof. J. Alex Halderman, and CDT at 4-6 (summarizing the record of supporting propositions), https://www.copyright.gov/1201/2018/comments-031418/class10/Class_10_Reply_Felten_Halderman_CDT.pdf.

[12] Specifically, CCIPS notes that it "supports making clear the research exemption would permit security research on devices regardless of whether they are primarily designed for use by individuals." CCIPS Letter at 4. Modifying 37 C.F.R. § 201.40(b)(7)(i)(A) to remove the "primarily designed for use by individual consumers" language would leave the exemption text to read: "Computer programs, where the circumvention is undertaken on a . . . device or machine on which the computer program operates, ... and the **device or machine is . . . (A) A device or machine** . . . " Given that a "device or machine" is always a "device or machine," the Device Limitation language would then be satisfied in every relevant circumstance and therefore superfluous. Accordingly, we read the CCIPS letter as implying support for removing the Device Limitation altogether.

[13] CCIPS Letter at 4.

includes."[14] CCIPS cites specific examples, including elevators, large-scale lighting, HVAC, and surveillance equipment, whose qualifications as "consumer" devices are unclear.[15] We agree.

CCIPS likewise emphasizes that "it is unclear what rationale there may be" for retaining the Device Limitation and that doing so "would seem to unnecessarily exclude valuable security research conducted on many classes of devices that, although arguably not 'primarily designed for use by individuals,' may nevertheless greatly affect individuals."[16] CCIPS highlights the importance of independent security research in discovering vulnerabilities in "[b]oth consumer-operated, network-enabled home appliances (often associated with the 'internet of things') and industrial-grade network routing and switching equipment," which "can pose threats to data security, critical infrastructure, and public safety," citing documented cases where it has "prosecuted . . . exploitation of vulnerabilities in both classes of equipment."[17] CCIPS emphasizes that "vulnerabilities contained in industrial grade servers or networking equipment may present even greater risks to the public than security flaws in consumer goods."[18] Again, we agree.

The Controlled Environment Limitation. Our comments explained in detail the ambiguities of the Controlled Environment Limitation and the potential chilling effect on legitimate research that cannot be conducted within the confines of a lab.[19] CCIPS again corroborates our view in support of its position that the Office should clarify or remove the limitation.[20]

More specifically, CCIPS "shares the concerns of petitioners that in its current form, the language of the Controlled Environment Limitation could be construed to suggest that, in order to fit within the exemption, security research must be conducted in a lab-like setting or other environment isolated from the public."[21]

---

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] Halderman and Felten Comment at 5, 21-23, 38; CDT Comments at 4; Halderman, Felten, and CDT Reply Comments at 15-17.

[20] *See* CCIPS Letter at 4.

[21] *Id.*

CCIPS "agree[s] . . . that in some circumstances effective research may require experiments to be conducted in realistic conditions in the field."[22] Again, we concur.

CCIPS suggests that, as a minimum, "it would be beneficial [for the Office] to clarify that, although exempted security research need not always be conducted in a laboratory setting, it must be conducted with reasonable consideration for risks of harm, or under conditions reasonably calculated to minimize risks to the public."[23]

We continue to believe that eliminating the Controlled Environment Limitation altogether is the best way to address its ambiguities. Introducing a reasonableness standard would still leave significant ambiguity about the ambit of the exemption for researchers who seek to be certain that their activities will be covered. Moreover, we reiterate that this rulemaking is an inappropriate forum in which to define the contours of appropriate security research; as CCIPS notes, "the DMCA's anti-circumvention provisions are not the most effective or appropriate vehicle for addressing concerns about security research methods."[24] In view of CCIPS' statement that it "would not object to [the] removal" of the Limitation, we urge the Office to follow the lengthy record established on this point and remove the limitation from the exemption.

Nevertheless, we agree with CCIPS that, if the Office insists on retaining some sort of environment limitation, a reasonableness-oriented formulation that requires research to "be conducted with reasonable consideration for risks of harm, or under conditions reasonably calculated to minimize risks to the public" would be preferable to the exemption's current language. If the Office recommends such a formulation, it should be codified only with statements from the Acting Register and Librarian that the standard is intended to be a low bar and not intended to suggest any significant but unstated requirements of or limitations on eligibility for the exemption.[25]

The Other Laws Limitation. Finally, our comments urged removal of the Other Laws Limitation, which we used as shorthand to refer to both the limitation that circumvention be undertaken on a "lawfully acquired device or machine on which the computer program operates" (the "*Lawfully Acquired Limitation*") and "not violate

---

[22] *Id.* at 4-5.

[23] *Id.* at 5.

[24] *See id.*

[25] *C.f. Whitman v. Am. Trucking Associations*, 531 U.S. 457, 468 (2001) ("[Congress] does not, one might say, hide elephants in mouseholes.")

any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986, as amended and codified in title 18, United States Code" (the "*Applicable Law Limitation*").[26]

The Lawfully Acquired Limitation. Our comments raised specific concerns about complex legal disputes unrelated to copyright law or the DMCA about whether a device is "lawfully acquired." We appreciate the recognition by CCIPS the "concern that this limitation could be read to exclude research on devices where ownership of the device is subject to restrictive licensing terms, or is disputed, or even where the device is merely owned by a third-party but never 'acquired' by the researcher."[27] We likewise agree with CCIPS that "the question of whether such research is permissible under the DMCA should not turn on restrictive contractual terms purporting to limit use of the hardware on which the copyrighted software is running."[28]

While we disagree with CCIPS' conclusion that the "lawfully acquired" language is salvageable and reiterate that the Office should recommend eliminating the limitation altogether, if the Office retains the limitation it should incorporate in the text of the exemption in the final rule and accompanying statements CCIPS' perspective that it does not read "the term in this context to require that researcher obtain formal title in a copy of software."[29] We concur with CCIPS that the "lawfully acquired" language, accompanied with a suitable clarification of its narrow scope, would be "less restrictive than, and preferable to, alternative limitations that would predicate permission to conduct research on ownership or formal acquisition of title in a particular copy of software or other work."[30]

The Applicable Law Limitation. Our comments highlighted the significant uncertainty introduced by importing the CFAA and other laws into the DMCA's significant federal civil and criminal penalty structures.[31] We agree with CCIPS' observation that

---

[26] *See* Halderman and Felten Comments at 2; *see also* CDT Comments at 4, 5.

[27] *See* CCIPS Letter at 5.

[28] *See id.*

[29] *See id.*

[30] *See id.* Of course, the Office's presumptive renewal of the existing exemption procedurally bars it from introducing an even more restrictive formulation of the limitation. *See* Exemptions To Permit Circumvention of Access Controls on Copyrighted Works, Notice of Proposed Rulemaking, 82 Fed. Reg. 49,550, 49,552, 49,562 (Oct. 26, 2017).

[31] Felten and Halderman Comments at 24; CDT Comments 4.

the reference to 'any applicable law' in the Limitation "does not change what is or is not permitted under other laws."[32] We also note that CCIPS "would not object to the removal of this phrase from the exemption" were it not linked to corresponding language requiring that exempt research not violate the Computer Fraud and Abuse Act (CFAA).[33]

At a bare minimum, even if the Office recommends retaining compliance with the CFAA as a prerequisite for eligibility for the exemption, the Office can easily (and should) square our position with CCIPS' by reformulating the exemption language to omit the reference to all other laws while retaining the reference to the CFAA. More specifically, the Office could simply remove the phrase "any applicable law, including without limitation," as follows:

> Computer programs, where the circumvention . . . 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; . . .

Of course, given the wide uncertainty about the applicability of the CFAA to many security research practices,[34] we disagree with CCIPS that conditioning eligibility for the security research exemption from Section 1201 on compliance with the CFAA makes for a wise policy choice.[35] However, we note that CCIPS raises only a very narrow concern about removing the reference to the CFAA from the Section 1201 exemption: that "[t]o do so might mislead researchers into believing that operating within the DMCA exemption would also provide an exemption from CFAA liability, which it does not."[36]

We believe the Office could adequately address this concern by removing the Applicable Law Limitation but including explicit language and/or a savings clause in both the language of the final rule and its corresponding discussion making clear that eligibility for the revised exemption from Section 1201 has no bearing on whether the exempted activity is consistent with the provisions of the CFAA.

As ambassadors and advisors to the security research community, we believe deliberate educational efforts by the Office, CCIPS, and participants in this

---

[32] CCIPS Letter at 6.

[33] *See id.*

[34] *See, e.g.*, Halderman, Felten, and CDT Comments at 23.

[35] *See* CCIPS Letter at 6.

[36] *See id.*

proceeding can succeed in conveying to the community the important distinction between the CFAA and the DMCA and the plain applicability of the proposed exemption to the latter but not the former.

* * *

Finally, we convey our appreciation to CCIPS for taking seriously the concerns of the security research community. Thank you again for the opportunity to comment. Please don't hesitate to contact us with any questions or concerns.

Respectfully submitted,

/s/

Ferras Vinh
Policy Counsel

Joseph Lorenzo Hall
Chief Technologist

Center for Democracy and Technology

fvinh@cdt.org

Blake Reid
Director

Samuelson-Glushko Technology Law & Policy Clinic (TLPC)

Counsel to Prof. Halderman

tlpc@colorado.edu

CC: John T. Lynch, DOJ
Leonard Bailey, DOJ
John Morris, NTIA