RAPID7

Jul. 13, 2018

Regan 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: Response to CCIPS letter on Proposed Class 10, Section 1201 Rulemaking (Docket No. 2017-10)

Dear Ms. Smith and Mr. Amer:

Thank you for the opportunity to respond to the important letter from the Computer Crime and Intellectual Property Section (CCIPS) of the U.S. Dept. of Justice on Proposed Class 10.[1] Rapid7 supports the Copyright Office's decision to include the letter in the record of the seventh triennial rulemaking proceedings. For purposes of this response, we focus on issues raised in both the CCIPS letter and Rapid7's previous comments to this rulemaking proceeding, specifically the "any applicable law" limitation to the security research exemption.[2]

Rapid7 agrees with the analysis of both CCIPS and the Register that other laws independently apply even if research is permissible under an exemption for good faith security research.[3] We also recognize the value of referencing this in the exemption text, to avoid the concern raised by CCIPS that researchers may mistakenly believe the exemption provides protection from other laws, such as the Computer Fraud and Abuse Act (CFAA).[4] Rapid7 would not object to an express reference to the CFAA, as CCIPS suggests, to highlight continued applicability of the CFAA independently of the security research exemption.

However, a reference to the applicability of other laws is distinct from making the security research exemption *contingent* on compliance with all other laws. The CCIPS letter does not call for the latter with regard to CFAA or other laws. An express reference to the fact that the security research exemption has no bearing on liability under other laws, without limiting the exemption to research that complies with all existing laws, will help prospective security researchers be reasonably sure whether their activities will be exempted. Such a modification to the exemption text would detract from neither to copyright nor security interests.

---

[1] Letter from the Dept. of Justice to the US Copyright Office, Jun. 28, 2018, https://www.copyright.gov/1201/2018/USCO-letters/USDOJ_Letter_to_USCO.pdf ("CCIPS letter").
[2] Joint comments of Rapid7, Bugcrowd, Duo Security, HackerOne, Luta Security to US Copyright Office Seventh Triennial Section 1201 Proceeding (2018) Class 10: Computer Programs—Security Research, Dec. 18, 2017, https://www.copyright.gov/1201/2018/comments-121817/class10/class-10-initialcomments-rapid7-et-al.pdf.
[3] CCIPS letter, pg. 5.
[4] *Id.*, pg. 6.

Accordingly, we suggest the Register modify the temporary security research exemption by striking in 37 CFR 201.40(a)(7)(i)

> "~~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 inserting in the definition of "good faith security research" in (iii)

> *good faith security research that qualifies for the security testing exemption may nevertheless incur liability under other applicable laws, including without limitation the Computer Fraud and Abuse Act of 1986, as amended and codified in title 18, United States Code.*

The CCIPS letter notes, and we agree, that Section 1201 is an inappropriate vehicle for mirroring the many prohibitions on illegal access or modification to devices or software beyond the protection of copyright interests.[5] As currently written, the "any applicable law" limitation to the security research exemption raises troubling issues researchers must grapple with. For example: if good faith security research violates obscure legal provisions with no bearing on security or copyright, but the relevant regulatory body does not pursue an enforcement action, would the security testing exemption nevertheless be forfeited and the researcher thereby exposed to a private right of action under 17 USC 1203(a)?

The "any applicable law" limitation creates uncertainty for rights-holders as well. For example, opponents of the petition to expand the security testing exemption warn that removal of the limitation would give "anonymous hackers a license to attack critical infrastructure"[6] or "hack into a flying aircraft,"[7] and result in "unfettered election hacking activities."[8] Yet, as the CCIPS letter notes and as has been repeatedly observed elsewhere, other laws enacted to directly constrain such activity would apply even if the "any applicable law" limitation were struck.

Two decades ago, when Congress deliberated on the "any applicable law" limitation in the 1201(j) permanent exemption for security testing, Congress focused on issues of consent and lawful acquisition, not the diversity of laws now implicated in an age of decentralized security

---

[5] *Id.*, pgs. 3, 5. "The fact that malicious tampering with certain devices or works could cause serious harm is reason to maintain legal prohibitions against such tampering, but not necessarily to try to mirror all such legal prohibitions within the DMCA's exemptions. [...] CCIPS also does not view the anti-circumvention provisions as the most appropriate or efficient means of imposing limits on security research beyond the scope of the copyright-related goals underlying the DMCA."

[6] Long comment of Election Systems Providers to Class 10, pg 4, https://www.copyright.gov/1201/2018/comments-021218/class10/Class_10_Opp'n_Election_System_Providers.pdf (last accessed Jul. 10, 2018).

[7] Long comment of The Software and Information Industry Association to Class 10, pg. 4, https://www.copyright.gov/1201/2018/comments-021218/class10/Class_10_Opp'n_SIIA.pdf (last accessed Jul. 10, 2018).

[8] Comment of the National Association of Secretaries of State to Class 10, Feb. 8, 2018, https://www.copyright.gov/1201/2018/comments-021218/class10/Class_10_Opp'n_National_Association_of_Secretaries_of%20State.pdf.

research on a vast array of software.[9] The triennial rulemaking process was designed to address such imbalances as technology evolved.[10] Today, mirroring the multitude of potential legal constraints on security research in the temporary exemption creates unnecessary uncertainty and a disproportionate penalty structure that advance neither copyright interests nor good faith security research.

* * *

We appreciate the opportunity to share our views. If there are additional questions or if Rapid7 can provide any further assistance, please contact Harley Geiger, Director of Public Policy, at Harley_Geiger[at]Rapid7.com. Thank you.

END

[9] H.R. Rep. No. 105-706, at 67 (1998) (Conf. Rep.). "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."

[10] H.R. Rep. No. 105-551, pt. 2, at 37 (1998) (Commerce Committee report).