UNITED STATES COPYRIGHT OFFICE

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

Rapid7 comments - Eighth Triennial Proceeding, Class 13

December 14, 2020

Item A. Commenter Information

Rapid7 is a cybersecurity and data analytics company headquartered in Boston, MA, with offices around the world. Rapid7 conducts and supports independent security research to advance the long-term security of all technology users, and as a complement to Rapid7's cybersecurity products and services. Rapid7 conducts security vulnerability testing on a variety of technologies, such as connected "Internet of Things" devices, and discloses discovered vulnerabilities to the technology manufacturers. In addition, Rapid7 helps coordinate the disclosure of vulnerabilities discovered by independent third party researchers to try to help them achieve optimal security outcomes. Rapid7's products and services manage cybersecurity risk, identify and reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Over 9,000 customers worldwide rely on Rapid7 technology, services, and research to improve cybersecurity outcomes, protect consumers, and securely advance their organizations.

In this proceeding, Rapid7 is represented by Harley Geiger, Director of Public Policy, harley_geiger@rapid7.com.

Item B. Proposed Class Addressed

Our comment focuses on the two petitions for Proposed Class 13, Computer Programs—Security Research.[1]

[1] 85 FR 65293

Item C. Overview

Rapid7 supports renewal of the current exemption for good-faith security research, but believes the language should be modified and clarified to avoid adverse effects on security research. Our comment addresses both petitions for Proposed Class 13:

1. The Halderman et. al petition. We recommend the Register modify the security research exemption to strike the "any applicable law" provision, and clarify the "used or maintained" provision, as proposed by the petition.

2. The Software Freedom Conservancy petition. We recommend that the Register clarify that the activities described in the Software Freedom Conservancy petition are already covered under the current exemption, and decline to modify the exemption.

Item E. Asserted Adverse Effects on Noninfringing Uses

1) The Halderman et. al petition

Rapid7 agrees with the Halderman et. al petition that several of the caveats in the temporary exemption create an adverse effect on security research by creating unnecessary uncertainty and risks that advance neither security research nor copyright interests.[2] We focus our comments on the recommendations to a) Remove the limitation that circumvention "not violate any applicable law;" and b) Ensure that researchers are not penalized for third party activities by the provision that information derived from the research "is not used or maintained in a manner that facilitates copyright infringement."

a) Remove the limitation that circumvention "not violate any applicable law."

The 2021 temporary exemption for security research should eliminate the redundant requirement of compliance with all other laws to be eligible for the exemption.[3] As noted by the Department of Justice, Sec. 1201 is an inappropriate vehicle for mirroring the many existing legal prohibitions on illegal access or modification to devices or software beyond the protection of copyright interests.[4] These other laws apply independently of section 1201, and

[2] Halderman, Center for Democracy & Technology, and Association of Computing Machinery, Petition for New Exemption Under 17 USC 1201, https://copyright.gov/1201/2021/petitions/proposed/New%20Pet.%20-%20J.%20Alex%20Halderman%20et%20al.pdf.
[3] 17 USC 1201(j)(2)-(3)(B). See also 37 CFR 201.40(b)(11)(i).
[4] Letter from the Dept. of Justice to the US Copyright Office, Jun. 28, 2018, pgs. 3-5, https://copyright.gov/1201/2018/USCO-letters/USDOJ_Letter_to_USCO.pdf. "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

violations carry their own penalties, remedies, and enforcement entities separate from copyright and the Librarian of Congress.[5] Rather than providing a clear safe harbor, the "any applicable law" provision creates adverse effects by requiring researchers to navigate unsettled law and complex jurisdictional issues, with potentially severe penalties for missteps. This increased and unnecessary burden falls heaviest on independent researchers without access to legal expertise or resources. These ambiguities and risks are inseparable from section 1201 so long as eligibility for the security research exemption depends on the "any applicable law" provision.

In its 2018 recommendation to the Seventh Triennial Rulemaking, the Register of Copyrights noted that Congress inserted the "any applicable law" provision into the statutory language of section 1201.[6] However, when Congress deliberated on the "any applicable law" limitation in the 1201(j) permanent exemption for security testing, Congress focused squarely on issues of consent and lawful acquisition.[7] The Copyright Office has already addressed consent and lawful acquisition elsewhere in the temporary exemption.[8] Two decades ago, Congress did not contemplate the broad diversity of laws now implicated in decentralized security research on a vast array of software, and how this would significantly expand the breadth of the "any applicable law" provision. This is the type of "flexibility in enforcement" issue that Congress intended the triennial rulemaking process to rebalance.[9]

In its 2018 recommendation to the Seventh Triennial Rulemaking, the Register also seemingly declined to remove the "any applicable law" requirement *because* researchers' conduct was constrained by other laws.[10] This creates an inconsistent and contradictory standard for researchers, as researchers have long argued that good faith research is fair use that merits an exemption under section 1201 in part because the research benefits society and does not intend to violate other laws.[11] Opponents of this change simultaneously warn the Register that

---

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."

[5] As the Register of Copyrights noted: "the rules that should govern [security research] are best considered by those responsible for our national security and for regulating the consumer products and services at issue." US Copyright Office, Section 1201 Rulemaking, Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendation of the Register of Copyrights, Oct. 2015, pg., 316, http://copyright.gov/1201/2015/registers-recommendation.pdf.

[6] Recommendation of the Acting Register of Copyrights, Seventh Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Oct. 2018, pg. 310-311, https://cdn.loc.gov/copyright/1201/2018/2018_Section_1201_Acting_Registers_Recommendation.pdf.

[7] 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."

[8] See 37 CFR 201.40(b)(11)(i). "[...] undertaken on a *lawfully acquired* device or machine […] with the *authorization* of the owner or operator of such computer."

[9] H.R. Rep. No. 105-551, pt. 2, at 36 (1998) (Commerce Committee report).

[10] Recommendation of the Acting Register of Copyrights, Seventh Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Oct. 2018, pg. 310.

[11] See, for example, discussion related fair use and the "controlled environment" limitation. Recommendation of the Acting Register of Copyrights, Seventh Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Oct. 2018, pgs. 292-298, 306-307.

removal of the “any applicable law” provision would prompt researchers to wildly violate other laws,[12] and yet also argue that the “any applicable law” provision should not be removed unless researchers demonstrate that they would disregard other laws if not for section 1201.[13] While the 2018 opponents are correct that section 1201 does not cause the ambiguity under other laws, these other laws are literally incorporated into section 1201 because of the “any applicable law” provision, thereby closely tying the effects of section 1201 with the ambiguities and risks of other statutes.

Researchers that seek to ensure protection under the current temporary exemption for security research are forced to weigh legal risks associated with the ambiguities of numerous obscure laws with uneven application in different jurisdictions. It is concerning that if good faith security research violates an obscure legal provision with no bearing on security or copyright, the security testing exemption may thus be forfeited and the researcher thereby exposed to private lawsuits under 17 USC 1203(a)(1)-(2).

For example, many Internet of Things (IoT) devices have a cloud or mobile app component, and security research may engage with these components (i.e., if the researcher buys the device and also uses the app).[14] Yet if terms of service or EULAs forbid research on the device, it is unclear whether the researcher’s use of the cloud or mobile app implicates the Computer Fraud and Abuse Act (CFAA). The extent to which a violation of terms of service is punishable under the Computer Fraud and Abuse Act (CFAA) is subject to a sharp split among US circuit courts and an active Supreme Court case.[15] Many state and local laws contain similar ambiguities and overbreadth.[16] Though the language of these statutes is the cause of this

---

[12] Opponents of the 2018 security research exemption warned that removal of the “any applicable law” limitation would give "anonymous hackers a license to attack critical infrastructure" or "hack into a flying aircraft," and result in "unfettered election hacking activities." Rights-holders have shown no evidence that removing the “any applicable law” limitation from the temporary exemption for security research would create these far-fetched outcomes. See Long comment of Election Systems Providers to Class 10, pg 4, https://copyright.gov/1201/2018/comments-021218/class10/Class_10_Opp'n_Election_System_Providers.pdf. See also Long comment of The Software and Information Industry Association to Class 10, pg. 4, https://copyright.gov/1201/2018/comments-021218/class10/Class_10_Opp'n_SIIA.pdf. See also Comment of the National Association of Secretaries of State to Class 10, Feb. 8, 2018, https://copyright.gov/1201/2018/comments-021218/class10/Class_10_Opp'n_National_Association_of_Secretaries_of%20State.pdf.

[13] See Recommendation of the Acting Register of Copyrights, Seventh Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Oct. 2018, pg. 310, https://cdn.loc.gov/copyright/1201/2018/2018_Section_1201_Acting_Registers_Recommendation.pdf.

[14] See, for example, Tod Beardsley, Multiple Hickory Smart Lock vulnerabilities, Aug. 1, 2019, https://blog.rapid7.com/2019/08/01/r7-2019-18-multiple-hickory-smart-lock-vulnerabilities.

[15] See Ronald Lee, Sixth Circuit Deepens Computer Fraud and Abuse Act Circuit Split, Arnold & Porter, Sep. 16, 2020, https://arnoldporter.com/en/perspectives/blogs/enforcement-edge/2020/09/sixth-circuit-deepens-cfaa-circuit-split. See also Ronald Mann, Justices to consider breadth of federal computer fraud statute, SCOTUSblog, Nov. 29, 2020, https://scotusblog.com/2020/11/case-preview-justices-to-consider-breadth-of-federal-computer-fraud-statute.

[16] For example, Maryland law states that a person may not possess, identify, or attempt to identify a valid access code without authorization. Maryland Criminal Code 7-302(c)(3). Yet weak default passwords and access codes are common security flaws in consumer devices. Maryland researchers would need to apply a complex and novel analysis of their liability under this law to ensure protection under the section 1201 exemption.

ambiguity, the impact of this ambiguity extends to Section 1201 through the “any applicable law” provision.

Non-US laws further complicate the ambiguities and risks for security researchers. Notably, Chinese-origin internet-enabled devices and device components are flooding the US market. Potential security flaws in these items and associated cloud-based features create well-recognized risks to supply chains and downstream consumer products.[17] It is often difficult or impossible to contact many of these manufacturers or software developers. At the same time, China has recently proposed multiple laws restricting independent researchers from disclosing vulnerabilities and security threat information - in sharp contrast to international standards and practice - raising alarms among US cybersecurity practitioners.[18] As noted by the practitioners’ comments, it is unclear how these proposed regulations are intended to apply to researchers, disclosures, or devices located outside China’s borders.[19] Yet failure to comply with applicable laws such as this would strip good faith researchers of protection under the “any applicable law” provision of the security research exemption.

The Register should act decisively to end the confusion, reduce adverse impacts caused by legal uncertainty on security testing, and provide a clear safe harbor for good faith researchers. We recommend replacing the “any applicable law” provision with a clarification that the security testing exemption does not void other applicable laws. Accordingly, we suggest the Register modify the temporary security research exemption by striking in 37 CFR 201.40(b)(11)(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 201.40(b)(11)(ii)

> *Good faith security research that qualifies for the exemption under paragraph (a) 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.*

[17] See, e.g., Cyberspace Solarium Commission, Building a trusted ICT supply chain, Oct. 2020, pgs. 1, 12-15, https://solarium.gov/public-communications/supply-chain-white-paper.
[18] See Cybersecurity Coalition and the Cyber Threat Alliance, Comments on “Cybersecurity Vulnerabilities Administrative Regulation, Jul. 17, 2019, pg. 2, https://cyberthreatalliance.org/wp-content/uploads/2019/07/Joint-Coalition-CTA-Letter-to-Ministry-of-Industry-and-Information-Technology-on-Draft-Cybersecurity-Vulnerabilities-Administrative-Regulation.pdf. See also Cybersecurity Coalition and the Cyber Threat Alliance, Enquiries on Management Measures for Cyber Security Threat Information Release, Dec. 18, 2019, https://cybersecuritycoalition.org/enquiries-on-management-measures.
[19] See Cybersecurity Coalition and the Cyber Threat Alliance, Comments on “Cybersecurity Vulnerabilities Administrative Regulation, Jul. 17, 2019, pg. 2.

b) Ensure that researchers are not penalized for third party activities by the provision that information derived from the research "is not used or maintained in a manner that facilitates copyright infringement."

Eligibility for the 2018 exemption is stripped if the information derived from the security testing "is used or maintained in a manner that does not facilitate infringement or any other applicable law."[20] However, the language of the exemption is ambiguous regarding who is using or maintaining the information.

Security researchers acting in good faith should not be penalized for unintended third party use of publicly disclosed information derived from the research activity. The results of security research are routinely published to aid awareness and correction of security vulnerabilities, and the information derived from security testing may be stolen or breached.[21] If a third party violates copyright using information intended for testing and correction of security flaws, the third party should be liable - not the security researcher.

The Register of Copyrights helpfully acknowledged this issue in its 2018 recommendation to the Seventh Triennial Rulemaking: "to address proponents' concern, the Acting Register now clarifies her understanding that this language refers to the researcher's own use and maintenance of the information derived from the research."[22] However, the actual language of the security testing exemption should reflect this clarification and resolve the ambiguity. We suggest the following modification to 37 CFR 201.40(b)(11)(ii):

> and *the person conducting security research does not use the information to facilitate* ~~not used or maintained in a manner that facilitates~~ copyright infringement.

[20] 37 CFR 201.40(b)(11)(ii)
[21] For example, the security testing tools and exploits of the cybersecurity firm FireEye were recently breached, putting those tools into the hands of third parties. See Kevin Mandia, FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community, Dec. 8, 2020, https://fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html.
[22] Recommendation of the Acting Register of Copyrights, Seventh Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Oct. 2018, pg 309.

2) The Software Freedom Conservancy petition

The SFC petition notes its proposal would be to "test for and investigate [...] functionality that inadvertently or deliberately exposes personally identifying information and other privacy-sensitive information to third parties."[23] Rapid7 believes the Software Freedom Conservancy (SFC) petition largely describes activities that are key to the concept of security testing. As such, we recommend the Copyright Office clarify that the existing statutory and regulatory exemptions cover these activities without change, and so no expansion or modification is necessary.

Here is a real-world example of a type of security research with strong privacy implications. In 2019, Rapid7 tested three children's GPS-enabled smart watches purchased from Amazon.[24] For this good faith security research, Rapid7 circumvented a faulty SMS text message filter and an extremely weak default password of "123456" hardcoded on the device. We discovered that exploiting these technical vulnerabilities could enable attackers to gain total control of the device. It proved impossible to contact all three of the watch manufacturers. The security risks posed by these vulnerabilities - i.e., exposing the user's geolocation and enabling third party contact with minors - are also standard privacy issues.[25]

Although the SFC petition refers to privacy, it should be noted that security has long been fundamental to privacy.[26] Exposure of personal or sensitive information is a common security risk, and the object of many instances of security research is the discovery of flaws or functionality that may result in exposure of personal or sensitive information. Please note also that though privacy generally implicates personal or sensitive information, security issues can extend beyond privacy to cover risks that do not implicate personal information, such as system failure or physical safety.[27]

Whether the exposure is inadvertent or deliberate should be immaterial so long as the other exemption criteria are met. Device makers' deliberate design choices, such as weak default passwords or unencrypted communication channels, may result in exposure of personal information that creates security and privacy risks for device users. Deliberate but inadequate measures to delete or minimize personal or sensitive information is another security

[23] Software Freedom Conservancy, Petition for New Exemption Under 17 USC 1201, https://copyright.gov/1201/2021/petitions/proposed/New%20Pet.%20-%20Software%20Freedom%20Conservancy%20-%202.pdf.
[24] Tod Beardsley, Vuln disclosure: Children's GPS smart watches, Rapid7, Dec. 11, 2019, https://blog.rapid7.com/2019/12/11/iot-vuln-disclosure-childrens-gps-smart-watches-r7-2019-57.
[25] Granular geolocation is commonly recognized as "personal information." See, for example, California Civil Code 1798.140(v)(1)(G) (as amended by the California Privacy Rights Act).
[26] See e.g., background of Fair Information Practice Principles: Department of Homeland Security, Privacy Policy Guidance Memorandum, Dec. 29, 2008, https://dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.
[27] See National Institute of Standards and Technology, NIST Privacy Framework 1.0, Jan. 16, 2020, pgs. 3, 6-7, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.

vulnerability with privacy implications.[28] Security researchers widely recognize that the concept of "good faith research" encompasses testing and investigation of such flaws to prevent exposure of personal or sensitive data. The existing security exemption criteria should be commonly understood to permit the same.

We suggest that the Copyright Office decline to modify the current security research exemption based on the SFC petition, and clarify in the Register's recommendation that the SFC petition, on its face, describes research activities consistent with the existing exemption. We recommend against modifying the security research exemption to create new nuances that will further confuse the security testing exemption, as this would be unnecessary.

* * *

We appreciate the opportunity to share our views. If there are additional questions or if Rapid7 can provide any further assistance, please do not hesitate to contact us.

[28] See, for example, Deral Heiland, Risks in disposing of IoT embedded technology, Rapid7, Apr. 28, 2020, https://blog.rapid7.com/2020/04/28/risks-in-disposing-of-iot-embedded-technology-2.