RAPID7 bugcrowd hackerone

Joint Comments to US Copyright Office Section 1201 Study (Docket No. 2015-8)

FIRST NAME: Harley
LAST NAME: Geiger
ORGANIZATION: Rapid7

DATE: Mar. 3, 2016

Rapid7, Bugcrowd, and HackerOne submit these joint comments to the Copyright Office's public study of Sec. 1201 of the Digital Millennium Copyright Act (DMCA).[1] We appreciate that the Copyright Office initiated this study and provided the opportunity to comment. In these comments, we focus on questions posed by the Copyright Office's notice of inquiry for which we have strong views because of our interests in security research. As the Copyright Office has already noted, we recognize that the Copyright Office is to an extent constrained by statute and that some changes to Sec. 1201 can only occur through legislative action.[2] We hope to continue working with the Copyright Office in the future on ensuring Sec. 1201 does not unnecessarily restrain beneficial security research.

Rapid7 is a cybersecurity analytics software and services company that helps organizations reduce the risk of a security breach, detect and investigate attacks, and build effective IT security programs. Identifying and addressing the vulnerabilities inherent in technical systems is a critical measure in mitigating cyber threats and reducing opportunities for attackers. Security research is fundamental to our ability to help our customers understand the risks they face and protect themselves, and we believe strongly in the value of independent security research for advancing cybersecurity.

Bugcrowd is a pioneer and innovator in crowdsourced security for the enterprise. Bugcrowd allows organizations to harness the creativity of more than 25,000 security researchers around the globe to identify and remediate critical software vulnerabilities.

HackerOne connects companies and the hacker community to build a safer Internet. HackerOne powers the leading vulnerability coordination platform, tapping into the power of the hacker community to reveal live vulnerabilities that require a company's immediate attention. Vulnerabilities surfaced by hackers help protect a company's brand and its user's information and data. With over 450 companies and more than 2,000 contributing hackers, HackerOne has the world's largest platform and community of its kind.

---

[1] Section 1201 Study: Notice and Request for Public Comment, U.S. Copyright Office, Library of Congress, 80 Fed. Reg. 81369, Dec. 29, 2015, http://copyright.gov/fedreg/2015/80fr81369.pdf.

[2] Statement of Maria Pallante, U.S. Register of Copyrights and Director of the U.S. Copyright Office, U.S. House of Representatives Committee on the Judiciary hearing on "The Register's Perspective on Copyright Review," 114th Cong., Apr. 29, 2015, http://judiciary.house.gov/_cache/files/1c82a3a6-3b1b-4a51-b212-281454d1e56e/written-testimony-of-register-maria-a-pallante.pdf.

1. ***Please provide any insights or observations regarding the role and effectiveness of the prohibition on circumvention of technological measures in section 1201(a).***

Sec. 1201 of the DMCA adversely affects good faith security research by forbidding researchers from circumventing technological protection measures (TPMs) to analyze software for vulnerabilities.[3] Researchers that do so are not seeking to infringe (or enable others to infringe) copyright, but rather seek to evaluate and test software for flaws that could cause harm to individuals and businesses.[4] Society would benefit – and copyright interests would not be weakened - by raising awareness and urging correction of such software vulnerabilities.

The risk of harm resulting from exploitation of software vulnerabilities can be quite serious. For example, as Rapid7 Senior Security Consultant Jay Radcliffe described in 2015 comments to the Copyright Office, urging an exemption for software security research, Sec. 1201 of the DMCA prevented him from evaluating security flaws in medical devices on which many lives depend.[5] In his comments, Radcliffe emphasized that the goal of the research was solely to enhance the safety of the devices, and the prospect of liability under Sec. 1201 for conducting the research ultimately leads to weaker security for the devices. Sec. 1201's significant civil and criminal penalties can especially chill independent researchers who lack regulatory expertise or ready access to legal counsel that can evaluate whether research may violate Sec. 1201.[6]

2. How should section 1201 accommodate interests that are outside of core copyright concerns, for example, in cases where circumvention of access controls protecting computer programs implicates issues of product interoperability or public safety?

We recommend that the Copyright Office accommodate non-copyright interests when issuing exemptions to Sec. 1201 under the triennial rulemaking process.[7] For example, good faith security research does not infringe copyright, and if the Office did not consider non-copyright concerns as part of its rulemaking process, there would be diminished opportunity to discuss the chilling effect Sec. 1201 has on security research. However, we recommend that the Copyright Office *not* accommodate non-copyright interests when *denying* an exemption to Sec. 1201.

Congress' purpose in enacting Sec. 1201 was to promote the availability of copyrighted works and

---

[3] 17 U.S.C. 1201.
[4] As the Copyright Office has previously concluded, security research is fair use. U.S. Copyright Office, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 37 C.F.R. 201, Oct. 28, 2015, pg. 48, http://copyright.gov/1201/2015/fedreg-publicinspectionFR.pdf.
[5] Jay Radcliffe, Comments on Proposed Class 25, Feb. 6, 2015, http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_Radcliffe_Class25.pdf.
[6] 17 U.S.C. 1203-1204.
[7] This is largely the case today under 17 U.S.C. 1201(a)(1)(C)(ii)-(iii).

protect rightsholders' copyright interests as they relate to copyrighted works.[8] Sec. 1201's application overshoots its purpose to the extent that Sec. 1201 restrains activity that does not implicate copyright interests, such as security research, and this should weigh in favor of the Office tailoring copyright regulations to unburden that activity – as it has in previous triennial rulemaking proceedings.

The purpose of Sec. 1201 is not – nor should it be – to protect non-copyright interests, such as public safety or emissions control, from activities that do not infringe copyright, such as security research. Yet opponents of security research exemptions to Sec. 1201, in urging denial of such exemptions, too often cite Sec. 1201 as necessary to advance or protect non-copyright interests. For example, several comments to the Copyright Office's triennial rulemaking opposing a security research exemption argued that an exemption would enable individuals to skirt vehicular safety and emissions standards.[9] Yet modifying a vehicle for this purpose would not be the goal of cybersecurity researchers, and such modifications are already prohibited by laws enacted for that very purpose.[10] Copyright law is not the appropriate means for aiding enforcement of non-copyright laws at the expense of security research, and non-copyright interests should not be considered in denying exemptions that thereby result in the use of copyright protection laws to advance interests wholly distinct from copyright.

When non-copyright activities, such as security research, are unnecessarily restrained by Sec. 1201, only the Copyright Office and Congress can be appealed to for corrective action. It is therefore appropriate for the Copyright Office to consider whether an exemption to Sec. 1201 should be issued or expanded to enable legitimate non-copyright activities. However, government bodies other than the Copyright Office are tasked with protecting non-copyright interests, such as vehicular safety and the National Highway Traffic Safety Administration or medical device safety and the Food and Drug Administration.[11] Entities that seek to advance non-copyright interests need not turn to copyright law or the Copyright Office to do so. The agencies with expertise and applicable missions can more directly regulate against the specific harms they seek to prevent, rather than forbidding the circumvention of technological protection measures to copyrighted works for non-infringing security research.

3. Should section 1201 be adjusted to provide for presumptive renewal of previously granted exemptions—for example, when there is no meaningful opposition to renewal—or otherwise be modified to streamline the process of continuing an existing exemption? If so, how?

---

[8] H.R. Rep. No. 105–551, pt. 2, at 23 (1998). See also, Staff of the H. Comm. on the Judiciary, 105th Cong., Section-by-Section Analysis of H.R. 2281 as Passed by the U.S. House of Representatives on Aug. 4, 1998, (Comm. Print 1998), pg. 6, http://digital-law-online.info/misc/HCommPrnt6.pdf.

[9] See, e.g., General Motors, Comments on Proposed Class 22, Mar. 27, 2015, pgs. 6-7, http://copyright.gov/1201/2015/comments-032715/class%2025/General_Motors_1201_2014.pdf.

[10] See, e.g., the Clean Air Act, 42 U.S.C. 7522(a), and the Motor Vehicle Safety Act, 49 U.S.C. 30122(b).

[11] As the Register noted: "The rules that should govern such [security] research hardly seem the province of copyright, since the considerations of how safely to encourage such investigation are fairly far afield from copyright's core purpose of promoting the creation and dissemination of creative works. Rather, the rules that should govern are best considered by those responsible for our national security and for regulating the consumer products and services at issue." The Register of Copyrights, Section 1201 Rulemaking: Sixth Triennial Proceeding, Recommendation of the Register of Copyrights, Oct. 2015, pg. 316, http://copyright.gov/1201/2015/registers-recommendation.pdf.

We recommend that Sec. 1201 be adjusted to establish a presumption in favor of renewal of the previously granted exemptions under Sec. 1201 for security research. The current triennial rulemaking process is complex and resource-intensive, especially for researchers without legal training or assistance, and creates uncertainty from one rulemaking to the next.

However, we urge against making the presumption of renewal contingent on a lack of "meaningful" opposition. As noted above, there is consistent opposition to a Sec. 1201 exemption for security research during triennial rulemaking processes, centered largely on protecting non-copyright interests. Fortunately, this opposition did not succeed in persuading the Copyright Office against adopting an exemption for security research, but the next triennial rulemaking is likely to evoke the same opposing arguments, which could preclude a presumption of renewal that hinged on lack of opposition.

Instead, we recommend that the presumption of renewal should be overcome by a considerably stronger standard than the original grant of the exemption, such as a material change in circumstances. In considering whether the presumption of renewal should apply to an exemption, we recommend (as noted above) that the Copyright Office weigh the extent to which the exemption is needed to protect and promote copyrighted works against the impact on non-copyright activity. However, we do not believe that advancing non-copyright interests should weigh in favor of denying an exemption – or rebutting a presumption of renewal of an exemption.

8. Please assess whether the existing categories of permanent exemptions are necessary, relevant, and/or sufficient. How do the permanent exemptions affect the current state of reverse engineering, encryption research, and security testing? [...] How might the existing permanent exemptions be amended to better facilitate such activities?

Rapid7 believes that the permanent exemption to Sec. 1201 for security testing is more beneficial than no exemption at all. However, Rapid7 agrees with the conclusion of the Copyright Office in 2015 that permanent exemptions in 17 U.S.C. 1201(j), 1201(f), and 1201(g) do not sufficiently protect and foster good faith security research.[12]

Language limiting the purpose of TPM circumvention in Sec. 1201(f), 1201(g), and 1201(j) hinders security research. Sec. 1201(f)(1) requires that circumvention be performed for the sole purpose of achieving interoperability, yet interoperability is not necessarily the purpose of security research. Similarly, 1201(g)(1)(A) requires that circumvention be performed to advance encryption, but security research does not necessarily involve encryption. Finally, Sec. 1201(j)(3)(A) requires consideration of whether information derived from security testing is used "solely" for promoting the security of the owner or operator of the computer system, yet security research may appropriately be undertaken for the benefit of software users or the broader public.

[12] U.S. Copyright Office, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 37 C.F.R. 201, Oct. 28, 2015, pgs. 48-49, http://copyright.gov/1201/2015/fedreg-publicinspectionFR.pdf.

The requirement in Sec. 1201(j)(1) that security researchers obtain authorization of owners or operators of computers prior to circumventing software TPMs can chill independent security research. If security research only takes place under circumstances dictated by the owner of the software, it may be difficult for the research to remain impartial, and the owner may prevent or delay publication of research that reflects negatively on the owner's software. As the digital ecosystem grows increasingly complex and interdependent, it can also be challenging to even determine who owns or operates a particular piece of software, which hinders obtaining authorization and applying the multifactor test in Sec. 1201(j)(3).

The requirement in Sec. 1201(j)(2) that the security testing not violate any other law creates additional ambiguity and risks for researchers. By conditioning Sec. 1201 liability for circumventing TPMs for security research on whether any other law is violated, the risks of noncompliance are compounded by adding Sec. 1201's penalties to the penalties of other laws. Yet security research can implicate numerous laws, with legal uncertainty and uneven application in different jurisdictions.[13] For example, the question of whether violation of terms of service is punishable under the Computer Fraud and Abuse Act is subject to a sharp split among US circuit courts.[14] Rather than providing a clear safe harbor, Sec. 1201(j) requires researchers to navigate unsettled law, complex jurisdictional issues, and potentially severe penalties for missteps.

We urge the Copyright Office to support legislation to strengthen the permanent exemption to security research under Sec. 1201(j) by 1) Removing the language requiring that the research be performed for the sole purpose of promoting the owner or operator of the computer system, 2) Removing the requirement that researchers obtain prior authorization of owners of the computer system, and 3) Removing the requirement that the research not violate any other laws.

* * *

We appreciate the opportunity to share our views, and would be pleased to discuss these and other recommendations further with Copyright Office staff. Thank you for your consideration.

END

[13] See Deirdre Mulligan et al., University of California, Berkeley School of Information, Statement on Legal Impediments to Cybersecurity Research, May 1, 2015, http://copyright.gov/1201/2015/hearing-exhibits/Cybersec-statement-5-21-15.pdf. See also, Aaron J. Burstein, Amending the ECPA to Enable a Culture of Cybersecurity Research," 22 Harv. J. Law & Tech., 2008, pg. 185 et seq., http://jolt.law.harvard.edu/articles/pdf/v22/22HarvJLTech167.pdf.

[14] See David Perera, Courts poised to reshape landmark computer crimes act, Politico, Feb. 17, 2016, http://www.politico.com/story/2016/02/courts-poised-to-reshape-landmark-computer-crimes-act-219402.