Joint Comments to US Copyright Office Notice of Inquiry (Docket No. 2015-8)

FIRST NAME: Harley
LAST NAME: Geiger
ORGANIZATION: Rapid7
DATE: Oct. 27, 2016

Rapid7, Bugcrowd, HackerOne, and Luta Security submit these joint comments to the Copyright Office's Sep. 27, 2016 notice of inquiry regarding 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. 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 from constantly evolving threats, 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 is the #1 bug bounty platform, connecting organizations with the world's largest community of highly-qualified hackers. More than 600 organizations, including The U.S. Department of Defense, General Motors, Uber, Twitter, GitHub, Kaspersky Lab, Square, Dropbox and the CERT Coordination Center trust HackerOne to find critical software vulnerabilities before criminals can

[1] Section 1201 Study: Request for Additional Comments, U.S. Copyright Office, Library of Congress, 81 Fed. Reg. 66296, Sep. 27, 2016, https://www.gpo.gov/fdsys/pkg/FR-2016-09-27/pdf/2016-23167.pdf.

exploit them. HackerOne customers have resolved more than 31,000 vulnerabilities and awarded more than $10,000,000 in bug bounties. HackerOne is headquartered in San Francisco.

Luta Security is the first and only company offering comprehensive vulnerability disclosure planning and bug bounty preparation that meets the defense goals and needs of governments and organizations. Founded by Katie Moussouris, the expert behind Microsoft Vulnerability Research, the creator of their first bug bounties, and the advisor who helped create the first bug bounty program of the United States government, called "Hack the Pentagon." Luta Security offers comprehensive assessments of organizational capabilities and recommendations for handling incoming vulnerability reports, following the ISO standards of which Ms. Moussouris is an author and editor. Governments and companies trust Luta Security to partner and plan for success in working with security researchers to improve their security.

1. The Copyright Office should not limit its inquiry or final recommendations to legislative reforms

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.[2] 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.[3] Society would benefit – and copyright interests would not be weakened - by raising awareness and urging correction of such software vulnerabilities. However, Sec. 1201's significant civil and criminal penalties can chill independent research, especially among researchers who lack regulatory expertise or ready access to legal counsel that can evaluate whether research may violate Sec. 1201.[4]

As it considers ways to address these issues, the Copyright Office should not be limited to legislative action alone. Although Rapid7 supports some changes to the statute that would require legislation, non-legislative changes can also make a positive impact. In particular, the Librarian of Congress should seek to implement, with or without new legislation, a presumption of renewal for temporary exemptions granted under the triennial rulemaking process. A presumption of renewal could be significantly helpful to reduce the complexity and resource intensity of the current triennial process, which requires exemption applicants to start over from scratch every three years.

In 2015 The Register of Copyrights indicated support for legislation encoding a presumption of renewal for temporary exemptions in cases with "no" opposition.[5] Although this support is helpful,

---

[2] 17 U.S.C. 1201.

[3] 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.

[4] See, e.g., Comments of Jay Radcliffe on Proposed Class 25, Feb. 6, 2015, http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_Radcliffe_Class25.pdf.

[5] 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.,

such a change to the triennial rulemaking process could be accomplished through the Librarian of Congress, without requiring Congress to amend the statute. 17 USC 1201(a)(1)(C) authorizes the Librarian of Congress to grant temporary exemptions through a triennial rulemaking, but the statute is silent on the required showing or burden of proof during this proceeding – both for granting exceptions and renewals of previously granted exceptions.[6] There is no statutory bar to creating a presumption of renewal for exemptions that have already been granted in prior rulemakings. Thus, while Rapid7 urges the Register to continue supporting legislation that streamlines the triennial process for renewing exemptions, Rapid7 also recommends that the Register initiate non-legislative action to achieve the same goal.

However, as we noted in previous comments to the Copyright Office, we urge against making the presumption of renewal contingent on a lack of "meaningful" opposition.[7] 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 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]

2. Responses to "Proposed Amendments to Existing Permanent Exemptions"

2.a: *"The Office is interested in commenters' views on whether [the 2015 temporary exemption for security testing] language would be appropriate for adoption as a permanent exemption, or whether there are specific changes or additional provisions that Congress may wish to consider."*

Rapid7 views the temporary exemption to Sec. 1201(a) for good faith security testing, as established in the 2015 triennial rulemaking, to be a significantly positive step for both cybersecurity generally and independent researchers seeking to protect consumers from harm.[9] Researchers' independence is severely constrained if the researchers must obtain the authorization of software copyright-holders for each act of research. The key benefit of the temporary exemption for security testing is that it clearly does not require good faith researchers to obtain authorization of the rightsholder to test software security on lawfully acquired devices.[10] This critical feature should not be altered if the temporary

---

Apr. 29, 2015, pg. 22, http://judiciary.house.gov/_cache/files/1c82a3a6-3b1b-4a51-b212-281454d1e56e/written-testimony-of-register-maria-a-pallante.pdf.

[6] See 65 Fed. Reg. 64558 (2000).

[7] Comments of Rapid7, Bugcrowd, and HackerOne to U.S. Copyright Office Sec. 1201 Study, Rapid7, Mar. 3, 2016, pg. 4, available at https://www.regulations.gov/document?D=COLC-2015-0012-0047.

[8] *Id.*, at 2-3.

[9] Jen Ellis, New DMCA Exemption is a Positive Step for Security Researchers, Rapid7, Oct. 28, 2015, https://community.rapid7.com/community/infosec/blog/2015/10/28/new-dmca-exemption-is-a-positive-step-for-security-researchers.

[10] 80 Fed. Reg. 65956.

exemption were to be incorporated into the permanent exemption for security testing.

However, a new permanent exemption for security testing should modify several other components present in the 2015 temporary exemption. Specifically:

i. **A security testing exemption to Sec. 1201 should not be contingent on compliance with all other laws. –** The 2015 temporary exemption for security testing appears to become void if the researcher violates any other laws, including the Computer Fraud and Abuse Act (CFAA).[11] Rapid7 recommends striking this portion of the language. We agree that the exemption does not obviate compliance with any other laws outside 17 USC 1201. However, the applicability of a Sec. 1201 exemption should not depend on whether laws outside Sec. 1201 are violated. Violations of other laws carry their own penalties, remedies, and enforcement entities separate from copyright and the Librarian of Congress.[12] If, for example, an act of research violates CFAA, the researcher could be sued privately or prosecuted criminally under CFAA,[13] and voiding the Sec. 1201 exemption due to a CFAA violation would largely have the effect of compounding penalties that are already strict under CFAA.[14] Security research can implicate numerous laws, with legal uncertainty and uneven application in different jurisdictions.[15] For example, the extent to which a violation of terms of service is punishable under the CFAA is subject to a sharp split among US circuit courts.[16] To avoid chilling good faith security research, the permanent exemption should provide a clear safe harbor, rather than requiring researchers to navigate unsettled law and complex jurisdictional issues, with potentially severe penalties for missteps.

ii. **A security testing exemption to Sec. 1201 should include broader categories of software. –** The 2015 temporary exemption for security testing limits the software that may be tested to, among other things, computer programs on "a device or machine primarily designed for use by individual consumers."[17] This limitation creates ambiguity regarding what software qualifies. For example, some devices are designed for use in both home and business environments, such as "small office/home office" (SOHO) routers and printers. Vulnerabilities

---

[11] *Id.* "...and does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act..."
[12] As the Register noted in 2015, “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://www.copyright.gov/1201/2015/registers-recommendation.pdf.
[13] 18 USC 1030(c), (g).
[14] See National Association of Criminal Defense Lawyers, Computer Fraud and Abuse Act (CFAA), https://www.nacdl.org/cfaa/ (last accessed Oct. 24, 2016).
[15] 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.
[16] 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.
[17] 80 Fed. Reg. 65956.

in such devices are capable of presenting significant risk to both individual consumers and businesses. We acknowledge the Librarian's rationale in seeking to exclude devices and software that can present safety issues or large-scale disruptions, but the temporary exception has other safeguards against these dangers – such as the requirement that the research take place in a controlled environment designed to avoid any harm.[18] One way to address this issue could be to modify the language to read "a device or machine designed for use by, but not limited to, individual consumers."[19]

iii. **A security testing exemption to Sec. 1201 should not penalize researchers for unintended third party uses of research results. –** The 2015 temporary exemption for security testing has a definition for "good faith security research" that forbids the information derived from research to be used or maintained in a manner that facilitates copyright infringement.[20] Rapid7 agrees that good faith security research does not seek to infringe copyright. Instead, the end goals of security research are typically to promote transparency of cybersecurity vulnerabilities that put consumers and businesses at risk, ideally prompting a patch or correction to the vulnerability. To achieve these goals, it is common practice for security researchers to disclose the results of research publicly,[21] including through the NIST National Vulnerability Database (NVD) and Common Vulnerabilities and Exposures (CVE) index of publicly known cybersecurity vulnerabilities.[22] Though the purpose of public disclosure and NVD/CVE is generally to prevent vulnerability exploitation by raising awareness and encouraging fixes, it is also possible for malicious actors to exploit known vulnerabilities. If a malicious actor exploits a known vulnerability for the purpose of violating copyright (such as by stealing copyrighted material from another computer), the researcher that discovered or publicly disclosed the vulnerability ("the information derived from research") should not be considered to have "facilitated copyright infringement." To avoid this scenario, the exemption language could be modified to read "where the information derived from the activity [...] is not primarily used or maintained for the purpose of facilitating copyright infringement." This modification should protect security testing information disclosed publicly for cybersecurity purposes, but exclude security testing information disclosed to enable infringement.

2.b: *"The exemption for security testing under section 1201(j) is limited to activities undertaken "with the authorization of the owner or operator of [the] computer, computer system, or computer network." [...] Please assess whether legislation may be appropriate in this area and discuss any specific legislative proposals that you believe should be considered."*

---

[18] *Id.*

[19] Of course, since technology will rapidly evolve, any legislative change should also preserve the triennial rulemaking process as a path for further expanding the categories of software applicable to future temporary security testing exemptions.

[20] 80 Fed. Reg. 65956,

[21] For example, it is the policy Rapid7 to privately disclose the results of research to the software vendor a minimum of 60 days before public disclosure to provide time for the vendor to mitigate the vulnerability. See Rapid7, Vulnerability Disclosure Policy, https://www.rapid7.com/disclosure.jsp (last accessed Oct. 24, 2016).

[22] Mitre, Common Vulnerabilities and Exposures, Oct. 21, 2016, https://cve.mitre.org.

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 class of software, which hinders obtaining authorization and applying the multifactor test in Sec. 1201(j)(3). Copyright law, including Sec. 1201, is an inappropriate legal tool for blocking unauthorized access to a computer or taking unauthorized actions on a computer – which are already broadly prohibited under the CFAA[23] – when such actions can provide social value without infringing copyright. At minimum, we recommend modifying the 1201(j)(1) requirement to explicitly exclude licensees of lawfully acquired software copies, so licensees that independently authorize good faith security testing on those copies are not penalized under Sec. 1201 (though the licensees may still be penalized under the terms of the license).

2.c: *"Section 1201(j) provides a two-factor framework to determine whether a person qualifies for the security testing exemption. [...] Some commenters advocated the removal of one or both of these factors from the statute. Please assess the advisability of such changes, or discuss any other specific legislative proposals you believe should be considered."*

17 USC 1201(j)(3)(A) requires consideration of whether the information derived from the security testing was used "solely" to promote the security of the owner or operator of the computer, or shared directly with the developer of such computer. Yet security research may appropriately be undertaken for the benefit of software users or the broader public, rather than "solely" to promote the security of the owner or operator of the computer. A better articulation can be adapted from the 2015 temporary exemption: "the information derived from the security testing is used primarily to promote the security or safety of the of devices, machines, systems, or networks on which the computer program operates, or those who use such devices, machines, systems, or networks." In addition, while sharing information derived from the research directly with the developer may be appropriate as a factor to consider, it should not be a requirement or the determining factor, as it is not uncommon for researchers to share only discovered vulnerabilities – for example, if the security test yields no results, the researcher may not contact the developer.

17 USC 1201(j)(3)(B) requires consideration of whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement or any other applicable law. Our assessment of this factor is articulated in 2.a.i-iii above, as this language is replicated in the 2015 temporary exemption for security testing. For the reasons noted above, we believe that applicability of security testing exemption to Sec. 1201 should not be contingent on compliance with all other laws, and that researchers acting in good faith should not be penalized for unintended third party use of publicly disclosed information derived from the research activity.

[23] 18 USC 1030(a)(2)(C).

* * *

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