UNITED STATES COPYRIGHT OFFICE

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

Item A. Commenter Information

Prof. J. Alex Halderman

Prof. Halderman is a computer scientist whose research focuses on computer security and privacy, emphasizing problems that broadly impact society and public policy, including software security, network security, data privacy, anonymity, electronic voting, censorship resistance, computer forensics, ethics, and cybercrime.

Represented by:

Samuelson-Glushko Technology Law & Policy Clinic • Colorado Law
Cara Groseth, Lucas Knudsen, and Wilson Scarbeary • Student Attorneys
Blake E. Reid • Director
blake.reid@colorado.edu

Center for Democracy and Technology (CDT)

CDT is a nonprofit public interest organization that supports laws, corporate policies, and technical tools to protect the civil liberties of Internet users and represents the public's interest in maintaining balanced copyright policies and a secure digital environment. CDT supports the clear and predictable application of laws and exemptions so that security researchers can perform beneficial research with certainty and has advocated for a broad exemption to Section 1201's prohibition on the circumvention of technological protection measures in the 2015 and 2018 triennial rulemakings.

U.S. Technology Policy Committee (USTPC) of the Association for Computing Machinery (ACM)

ACM (the Association for Computing Machinery) is the world's largest educational and scientific computing society. The ACM U.S. Technology Policy Committee (USTPC) serves as the focal point for ACM's interaction with the U.S. government in all matters of U.S. public policy related to information technology. USTPC's membership is comprised of individual computer scientists, educators, researchers, and other technology professionals. In the sixth triennial rulemaking, ACM's U.S. policy committee (renamed USTPC in 2018) strongly endorsed and documented the need for a new security research exemption to Section 1201 of the Digital Millennium Copyright Act (DMCA) in 2015 comments to the Copyright Office. Subsequently, in a 2017 filing in the last such proceeding, the Committee urged both renewal and expansion of that exemption. ACM first formally engaged with the Copyright Office on the matter of DMCA exemptions in February of 2000.

Table of Contents

Item B. Proposed Class Addressed Class 13: Computer Programs—Security Research

On October 15, 2020 the Office issued a Notice of Proposed Rulemaking announcing its intention to renew the existing security research exemption to the anticircumvention provisions of the Digital Millennium Copyright Act, codified at 37 C.F.R § 201.40(b)(11).[1] The Office also sought comment from proponents on proposed expansions to exemptions, including the security research exemption.[2] On December 15, we filed comments asking the Office to expand the security research exemption.[3]

Item C. Overview

In our long comment, we asked the Office to remove both the Use and Other Laws Limitations that currently adversely impact security research.[4] The Use Limitations cabin the security research exemption through ambiguous terms including "solely" and "primarily" that create uncertainty for security researchers concerning their ability to participate in post-circumvention conduct including scholarship and criticism.[5] The Other Laws Limitations include extraneous references to non-copyright legal regimes that turn Section 1201 into an omnibus tool of cybersecurity policy, outside of the limited purpose of protecting copyright.[6] As we indicated, removing these limitations is consistent with all of the fair use factors as well as a majority of statutory factors laid out at 17 U.S.C. 1201(a)(1)(C).[7]

---

[1] Exemptions to Permit Circumvention of Access Controls on Copyrighted Works, 85 Fed. Reg. 65,293 (Oct. 15, 2020) (2020 NPRM),https://www.govinfo.gov/content/pkg/FR-2020-10-15/pdf/2020-22893.pdf.

[2] *See id*. at 65,300-301.

[3] Long Comment of Prof. J. Alex Halderman, Center for Democracy and Technology, and the U.S. Technology Policy Committee of the Association of Computing Machinery, Docket No. 2020-11 (Dec. 14, 2020) (Long Comment), https://www.copyright.gov/1201/2021/comments/Class%2013_InitialComments_J.%20Alex%20Halderman,%20Center%20for%20Democracy%20&%20Technology,%20and%20U.S.%20Technology%20Policy%20Committee%20of%20the%20Association%20for%20Computing%20Machinery.pdf.

[4] *See id*.

[5] *Id.* at 5

[6] *Id.*

[7] *Id.* at 12-35.

Rather than contesting this, opponents argue that striking these limitations would facilitate copyright infringement[8] or raise a variety of other speculative concerns around non-copyright issues such as threatening their business models, easing industrial espionage, or threatening bug bounty programs.[9] Opponents have provided no evidence beyond baseless speculation—nor is there any reason to expect—that these concerns are likely to materialize. Our proposed modifications largely preserve the existing definition of "good faith security research", which categorically excludes any conduct that amounts to or facilitates infringement. Moreover, our proposed modifications do not change the applicability of other existing legal remedies that are available to protect the rights of copyright holders. Our proposed modifications will simply eliminate ambiguities with the existing exemption that creates uncertainty for security researchers.

Alternatively, some opponents argue that the Office should maintain the limitations for the same reasons it did in the 2018 rulemaking.[10] Opponents largely fail to grapple with any of the new evidence we raised that weighs in favor of granting our proposed modifications to track developments in both the common law and the cybersecurity ecosystem.[11]

---

[8] *See* Comments of ACT at 3 (Feb. 9, 2020), https://www.copyright.gov/1201/2021/comments/opposition/Class_13_Opp'n_ACT%20The%20App%20Association.pdf; Comments of MPA, et al. at 5 Docket No. 2020-11 (Feb. 9, 2020), https://www.copyright.gov/1201/2021/comments/opposition/Class_13_Opp'n_Joint%20Creators%20and%20Copyright%20Owners.pdf ("Joint Copyright Holders Comment"); Comments of the Software and Information Industry Association (SIIA) at 2, 5 (Feb. 9, 2020), https://www.copyright.gov/1201/2021/comments/opposition/Class_13_Opp'n_Software%20and%20Information%20Industry%20Association.pdf.

[9] ACT Comment at 2-4.

[10] Comments of BSA at 3-6 (Feb. 9, 2020), https://www.copyright.gov/1201/2021/comments/opposition/Class_13_Opp'n_BSA%20The%20Software%20Alliance.pdf; Comments of the Motor & Equipment Manufacturers Association (MEMA) at 2 (Feb. 9, 2020), https://www.copyright.gov/1201/2021/comments/opposition/Class_13_Opp'n_The%20Motor%20&%20Equipment%20Manufacturers%20Association%20FINAL.pdf; Comments of DVD CCA and AACS LA at 4 (Feb. 9, 2020), https://www.copyright.gov/1201/2021/comments/opposition/Class_13_Opp'n_DVD%20CCA%20and%20AACS%20LA.pdf; ACT Comment at 2; Joint Copyright Holders at 4; SIIA Comment at 3.

[11] See Long Comment at 19-20 (discussing the constitutional issues implicated by *Green v. Dept. of Justice*, 392 F.Supp.3d 68 (D.D.C. 2019)).

The record is unanimous that security research plays a vital role in our cybersecurity architecture.[12] Removing the ambiguities with the existing exemption is necessary to ensure that independent security researchers can confidently contribute to this endeavor.

Item D. Technological Protection Measure(s) and Method(s) of Circumvention

As we noted in our long comment, the record in previous triennial rulemakings has well established that TPMs and the prohibition against circumventing them are detrimental to good-faith security research.[13] As Prof. Halderman pointed out in 2018 rulemaking, the Register found in 2015 that "TPMs protecting computer programs have a substantial adverse impact on good-faith testing for and the identification, disclosure and correction of malfunctions, security flaws and vulnerabilities in the protected computer programs."[14] As the Office has recommended the exemption for renewal—a decision that no opponent contests—the record is unanimous that TPMs are detrimental to good-faith security research.[15]

Item E. Asserted Adverse Effects on Noninfringing Uses

I. The record supports removing the Use Limitations.

The Use Limitations unnecessarily cabin the security research exemption in ways that provide uncertainty for security researchers in their ability to freely discuss and share their work without fear of liability.[16] The fair use and statutory factors cut in favor of removing these limitations.[17] To facilitate vital security research, the Office should remove the Use Limitations.[18]

---

[12] E.g., Long Comment at 8-11; Comments of HackerOne at 2 (Dec. 14, 2020), https://www.copyright.gov/1201/2021/comments/Class%2013_InitialComments_HackerOne.pdf; ACT Comment at 3.

[13] *See generally* Long Comment of Prof. Ed Felten and Prof. J. Alex Halderman, Docket No 2017-10 (Dec. 18, 2017) ("2018 Comment") https://cdn.loc.gov/copyright/1201/2018/comments-121817/class10/class-10-initialcomments-felten-halderman.pdf.

[14] *Id.* at 6-7 (quoting Recommendation of the Register of Copyrights at 305 (Oct. 8, 2015) (2015 Recommendation), https://www.copyright.gov/1201/2015/registers-recommendation.pdf)).

[15] 2020 NPRM at 65,300-01.

[16] Long Comment at 5.

[17] *Id.* at 12-35.

[18] In our long comment, we outlined the various legal uncertainties caused by the current security research exemption. *See* Long Comment at 18-23. This uncertainty leaves researchers with an untenable choice: conduct research publicly and face the

a. The record is clear that the Use Limitations create untenable ambiguity for security researchers.

In our long comment, we established that the current exemption raises ambiguities about whether security researchers can be held liable for post-circumvention conduct that is uncontroversially a fair use.[19] The record is unanimous that security research, including discussion, publication and peer review of the results constitutes a fair use.[20]

However, as other commenters note, the current exemption creates problematic uncertainty for security researchers. HackerOne explains that the current exemption in antithetical to the very purpose of security research because it discourages researchers from sharing their work or pushing the boundaries of the field.[21] According to HackerOne, researchers frequently conduct security testing for other valid purposes—such as testing their own skills or advancing the field.[22] HackerOne also points out that malicious actors can take advantage of a security researcher's good faith disclosure to exploit a vulnerability for criminal gain.[23] In these cases, security researchers may be reluctant to share or discuss their work for fear of liability.

Rapid7 agrees that the existing exemption punishes security researchers for behavior that is entirely outside of their control.[24] Rapid 7 explains that as written, the current exemption also requires that the information accessed is "not used or maintained in a manner that facilitates infringement."[25] Rapid7 notes that this condition could expose a security research to liability where a subsequent malicious actor leverages information in a vulnerability disclosure to commit copyright

---

potential for unjustified retaliation, or not perform it all, denying the public the benefit of the research.

[19] Long Comment at 18-23.

[20] *See* Long Comment at 14-17; Comments of the Software Freedom Conservancy (SFC) at 6-7 (Dec. 14, 2020), https://www.copyright.gov/1201/2021/comments/Class%2013_Initial%20Comment_Software%20Freedom%20Conservancy.pdf; Comments of Rapid7 at 3(Dec. 14, 2020), https://www.copyright.gov/1201/2021/comments/Class%2013_InitialComments_Rapid7.pdf.

[21] HackerOne Comment at 4.

[22] *Id*.

[23] *Id*. at 5.

[24] Rapid7 Comment at 6.

[25] *Id*. (citing 37 C.F.R § 201.40(b)(11)(ii)).

infringement.[26] Rapid7 argues, and we agree, that removing this condition on the exemption is necessary to provide clarity to security researchers.[27]

b. The record is clear that removing the Use Limitations is necessary guarantee the constitutional rights of security researchers.

Our long comment outlined the various unresolved legal questions created by the Use Limitations.[28] Opponents do not engage with the substance of any of these arguments, and simply ask the Office to double down on vague clarifications it has previously issued.[29]

BSA and the Joint Copyright Holders both point to a purported clarification issued by the Office that resolves the issues with the Use Limitations.[30] This clarification—issued during the 2018 Rulemaking—merely notes that "primarily" and "only" are not synonymous, and that a copyright holder had pursued charges against a researcher under such a theory.[31] The Office's clarification did not fully address the issues we identified with the Use Limitations; security researchers face continued uncertainty in their ability to engage in scholarship and criticism. Moreover, the clarification relied upon by BSA and the Joint Copyright Holders was issued well before *Green v. Dept. of Justice* was decided, indicating that further

[26] Rapid7 Comment at 6.

[27] *Id.*; Long Comment at 18-23.

[28] Long Comment at 18-23.

[29] SIIA also asks the Office to consider the impacts of the Supreme Court's "recent Eleventh Amendment jurisprudence" and condition the applicability of an exemption under Section 1201 on the presence of a waiver of state sovereign immunity. SIIA Comment at 2. SIIA's conclusory request neglects to provide any citations to case law or concrete legal argument, much less provide any explanation for how Section 1201 could give the Office the authority to impose such an apparently unconstitutional limitation on an exemption. Regardless, many security researchers do not work for state institutions and are not shielded by sovereign immunity. The Office should reject this request accordingly; if it chooses to allow SIIA to elaborate at the hearing or otherwise, it should provide all commenters opportunity to respond.

[30] BSA Comment at 3-4; Joint Copyright Holders Comment at 3-4.

[31] Recommendation of the Acting Register of Copyrights at 286 (Oct. 2018) (2018 Recommendation), https://cdn.loc.gov/copyright/1201/2018/2018_Section_1201_Acting_Registers_Recommendation.pdf.

guidance may be necessary to ensure that the exemption tracks developments in the common law.[32]

In our long comment, we discussed at length the issues raised by *Green*,[33] but opponents do not actually engage with the substance of any of these arguments. Rather, the DVD Copy Control Association simply insists that our reading of *Green* is "implausible," providing no legal analysis to support its argument.[34] Even given that the *Green* court was deciding a motion for summary judgment, the court came to the inescapable legal conclusion that Section 1201 may impermissibly limit the First Amendment rights of security researchers.[35]

Moreover, not only is our reading of *Green* entirely plausible, but it is bolstered by the record. Other proponents note that—as drafted—the security research exemption does not sufficiently protect security researchers from the possibility of litigation following good-faith vulnerability disclosures. As Rapid7 notes, security researchers face the potential for retaliatory litigation following a good-faith disclosure that is subsequently exploited by a bad actor.[36] HackerOne also asks the Office to correct this issue with the current exemption so researchers can freely share and discuss their work.[37] The Office should listen to this consensus of stakeholders rather than endorsing threadbare legal conclusions.

c. Removing the Use Limitations will address the bulk of the issues raised by the Software Freedom Conservancy.

The Software Freedom Conservancy (SFC) correctly notes that certain areas of privacy research—such as determining whether an application contains vulnerabilities that allows for access to private information—do not fall neatly within the bounds of the existing exemption.[38] Simply removing the Use Limitations would be the best way of resolving this ambiguity. As we noted in our initial comments, doing so will ensure that security researchers are allowed to engage in the full spectrum of privacy and security testing with certainty about their risk of liability.[39] These modifications are also in line with NTIA's

---

[32] *See* Long Comment at 19-20 (discussing the constitutional issues implicated by the *Green* case).

[33] *Id*. at 8-9, 18-21.

[34] DVD CCA & AACS LA Comment at 3.

[35] Long Comment at 19 (citing *Green at* 96).

[36] Rapid7 Comment at 6.

[37] HackerOne Comment at 4-5.

[38] SFC Comment at 2.

[39] Long Comment at 18-23

recommendation that the Office outline clear exceptions that are not overly complicated.[40]

SFC also asks the Office to expand the definition of good faith security research to include allowing consumers to make privacy-enhancing modifications to their own devices.[41] SFC raises compelling arguments in support of this proposition, but this class of conduct does not fit neatly within the definition of security research. This class of conduct would be best considered as its own class separate from security research, or perhaps under an expansion of the Repair, Unlocking, or Jailbreaking exceptions.[42] Depending on SFC's and the Office's preferences, we would be happy to provide further input.

II. The record supports removing the Other Laws Limitations

The Other Laws Limitations condition the applicability of an exemption on non-copyright legal regimes.[43] These limitations create a potential mechanism for copyright holders to deter conduct that would otherwise be considered a valid fair use simply because it paints their products in a negative light.[44]

a. Security researchers still face significant legal risks, even if their work is well supported.

Our long comment established that removing the Other Laws Limitations is warranted under the majority of the statutory factors in Section 1201 as well as the fair use factors.[45] No commenter contests this weight of authority.[46] Instead,

---

[40] Recommendations of the National Telecommunications and Information Administration to the Register of Copyrights at 4 (2018 NTIA Recommendation), https://www.ntia.doc.gov/files/ntia/publications/ntia_dmca_consultation_09252018.pdf.

[41] SFC Comment at 4-5.

[42] *See* 2020 NPRM at 65,299-300 (discussing the Repair exemptions); also see 202 NPRM at 65,306-7 (discussing the Unlocking and Jailbreaking exemptions).

[43] Long Comment at 5.

[44] *Id.* at 24-29.

[45] *Id.* at 12-35.

[46] ACT insists that because application companies rely on TPMs to limit access to certain information in order to comply with various privacy regulations, it is "impossible" to isolate the DMCA from non-copyright legal regimes. *See* ACT Comment at 4. To be clear, removing the linkage between the Section 1201 and "all other laws" won't materially affect the ability of companies to continue to secure their products with TPMs to comply with various regulations. It would merely constrain the reach of Section 1201 to copyright concerns. *See* Long Comment at 29.

opponents insist that because Congress also included similar language in the permanent exemptions, removing this language is unwarranted.[47]

However, Congress explicitly added the triennial review process to Section 1201 to allow the Office to adjust and rework exemptions based on changing circumstances and new technologies.[48] Constraining the temporary exemptions to the text of the exceptions in the original statute is thus entirely antithetical to the purpose of the triennial review. Moreover, as we noted in our initial comments, tying the applicability of an exemption to legal regimes outside of copyright stretches the bounds of the Progress Clause.[49] Opponents do not dispute or even address this analysis.

ACT additionally argues that because security researchers are well-supported by some firms, removing the Other Laws and Use Limitations is not warranted.[50] But simply receiving funding for their work does not make the threat of litigation speculative or harmful for researchers. Opponents essentially argue that because security research is well-supported by some companies, no researchers anywhere need to worry about the Sword of Damocles dangling above their heads.

The reality is that while security research is becoming more well-supported, some firms still remain hostile to disclosures concerning vulnerabilities in their products.[51] Indeed, we pointed to incidents where good-faith researchers have faced retaliation for reporting on vulnerabilities in compliance with a firm's disclosure policy.[52] Removing the Other Laws Limitations—which create potential these kinds of retaliatory claims—remains the best way to support security research.

---

[47] ACT Comment at 2-3; BSA Comment at 6; Joint Copyright Holders Comment at 6; SIAA Comment at 4

[48] *See* 17 U.S.C. §1201(a)(1).

[49] Long Comment at 28.

[50] ACT Comment at 3.

[51] Long Comment at 9-10, 35-37. In our long comment, we pointed to election machine vendors as one type of developer that has been hostile to security research. *See* Long Comment at 10, 21-23, 37. Since our long comment, researchers have identified additional vulnerabilities in election machine software that would allow these systems to be manipulated in ways that would be untraceable. *See* Andrew Appel and Susan Greenhalgh, *Voting Machine Hashcode Testing: Unsurprisingly insecure, and surprisingly insecure*, Freedom to Tinker (Mar 5, 2021) https://freedom-to-tinker.com/2021/03/05/voting-machine-hashcode-testing-unsurprisingly-insecure-and-surprisingly-insecure/.

[52] Long Comment at 22.

b. Removing the Other Laws Limitations will not create a back door to infringement

When malicious actors knowingly commit copyright infringement, adequate remedies exist to protect the rights of copyright holders. Copyright holders can pursue claims subsequent to their rights under 17 U.S.C. § 106 again any infringer—including security researchers who *actually commit* infringement. Numerous comments insist that by striking the requirement that information not be "used or maintained in a manner that facilitates infringement" will create a back door to infringement that will leave holders unable to protect their copyright.[53]

While opponents insist that these protections are necessary, not a single commenter has provided an example of an instance where Section 1201 has prevented them from being able to vindicate their rights in court where circumvention of a TPM enabled unauthorized reproduction or distribution of copyrighted content. Additionally, in hearings before Congress convened to explore reforms to Section 1201, proponents advanced similar arguments without providing any legal or factual support to those claims.[54]

Removing the Other Laws Limitation would not materially limit copyright holders from pursuing claims against would-be infringers who directly facilitate infringement—or cause other non-copyright harms.[55] But as we noted in our initial comments, removing this language is essential to provide the clarity security researchers need to properly conduct their work.[56]

---

[53] ACT Comment at 3; SIAA Comment at 2

[54] *See Are Reforms to Section 1201 Needed and Warranted? Before the Subcommittee on Intellectual Property of the Senate Committee on the Judiciary*, 116th Cong. at 11-13 (2020) (Response of Blake Reid to questions submitted for the record) (Reid 2020 QFR Response), https://www.judiciary.senate.gov/imo/media/doc/Reid%20Responses%20to%20QFRs.pdf.

[55] *See* Long Comment at 29. Additionally, the Motor & Equipment Manufacturers Association claims that in the context of motor vehicles, the Office should be more exacting and draw narrower exceptions to protect public safety. MEMA Comments at 2. But this argument was specifically rebuffed in 2018 when the Register decided to do away with the Device Limitation and update the exemption to apply equally to all kinds of software programs, regardless of the devices they run on. *See* 2018 Recommendation at 289.

[56] Long Comment at 23-29.

c. Limitations to the exemption, if any, must be grounded in copyright law.

As we noted in our long comment, the current exception contains problematic references to non-copyright legal regimes that create uncertainty for security researchers.[57] Rapid7 agrees that the Other Laws Limitation introduces uncertainty for security researchers and unnecessarily expands the inquiry concerning exemptions from copyright into extraneous legal regimes.[58] However, Rapid7 asks the Office to take a slightly different tack concerning the Other Laws Limitation: replacing the existing language with a disclaimer that researchers, "may nevertheless incur liability under other applicable laws, including without limitation the Computer Fraud and Abuse Act . . . . "[59]

We continue to believe that fully striking any reference to non-copyright legal regimes is the ideal formulation for exemption language. Doing so would accord with NTIA's 2018 recommendation that the Office focus exemption requirements "only" on copyright law.[60] However, Rapid7's proposed modification with regard to the Other Laws Limitation would solve many of the issues with the Other Laws Limitation.

[57] *Id*.

[58] Rapid7 Comment at 2-5.

[59] *Id*. at 5.

[60] 2018 NTIA Recommendation at 4.