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

The Copyright Office initiated the eighth triennial rulemaking to consider exemptions from the anticircumvention provisions of the Digital Millennium Copyright Act (DMCA) on June 22, 2020 by issuing a Notice of Inquiry and Request for Petitions.[1] In response, the above-signed petitioners filed a petition to renew the existing exemption for good-faith security research under Rule 201.40(b)(11) on July 16, 2020[2] and a petition to modify the exemption on September 8, 2020.[3] On October 15, 2020, the Copyright Office issued a Notice of Proposed Rulemaking (NPRM) for this proceeding.[4]

In the NPRM, the Office announced that it "intends to recommend renewal" of the existing good-faith security research exemption.[5] The current exemption applies to circumvention undertaken under the following conditions:

> (i) Computer programs, where the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates, or is undertaken on a computer, computer system, or computer network on which the computer program operates with the authorization of the owner or operator of such computer, computer system, or computer network, solely for the purpose of good-faith security research and does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986.
>
> (ii) For purposes of this paragraph (b)(11), "good-faith security research" means accessing a computer program

---

[1] Exemptions to Permit Circumvention of Access Controls on Copyrighted Works, 85 Fed. Reg. 37,399 (Jun. 22, 2020) (2020 NOI). https://www.govinfo.gov/content/pkg/FR-2020-06-22/pdf/2020-12911.pdf .

[2] Renewal Petition of J. Alex Halderman et al. (2020 Renewal Petition), https://www.copyright.gov/1201/2021/petitions/renewal/Renewal%20Pet.%20-%20Security%20Research%20-%20Halderman,%20CDT,%20ACM.pdf.

[3] Our modification petition erroneously cited to Rule 201.40(b)(7), and not (b)(11), as the codification of the temporary exemption for security research. *See* Modification Petition of J. Alex Halderman et al. (2020 Modification Petition) https://www.copyright.gov/1201/2021/petitions/proposed/New%20Pet.%20-%20J.%20Alex%20Halderman%20et%20al.pdf. We clarified this citation with the Office via email.

[4] 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.

[5] *Id.* at 65,300-301.

> solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in an environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement.[6]

We appreciate the Office's decision to recommend renewal of the existing exemption. Renewing the existing exemption is a positive step toward enabling security research.

However, the current exemption continues to create significant uncertainty for researchers around what kinds of post circumvention conduct—like scholarship and criticism—may impact the applicability of Section 1201. Additionally, the current exemption imports uncertainty from legal regimes outside of copyright law—such as the Computer Fraud and Abuse Act (CFAA)—creating additional confusion for security researchers and unnecessary complexity for the Office in administering these rules.

To guarantee that researchers can continue to engage in beneficial, noninfringing good-faith security research, and simplify the process for evaluating alleged violations, the Library and the Office should modify and clarify the existing exemption by removing:[7]

---

[6] 37 C.F.R § 201.40(b)(11).

[7] The Office sought comment on these proposed changes. 2020 NPRM, 85 Fed. Reg. at 65,307. The Office also sought comment on the petition of the Software Freedom Conservancy (SFC), which requested modifications of the current temporary exemption relating to "good-faith testing, investigation, and/or correction of privacy issues" and the ability to "remove software or disable functionality that may expose personal information," Modification Petition of SFC at 2 (Sept. 8, 2020) https://www.copyright.gov/1201/2021/petitions/proposed/New%20Pet.%20-%20Software%20Freedom%20Conservancy%20-%202.pdf. 2020 NPRM, 85 Fed. Reg. at 65,307 We will defer comments on SFC's petition to the reply round in anticipation of SFC further clarifying and explaining the details of its petition in its comments.

1. The "**Use Limitations,**" including:
    a. The "**Purpose Limitation,**" which includes both references to the term "solely" from the provisions of the exemption. The Purpose Limitation cabins the exemption to circumvention undertaken "solely for the purpose of good-faith security research," and that limit good-faith security research to accessing a computer program "solely for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability."[8]
    b. The "**Security Limitation,**" which requires that "the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement."[9]
2. The "**Other Laws Limitations,**" which unnecessarily condition eligibility for the exemption upon various legal regimes unrelated to protecting copyright, including:
    a. The "**Lawfully Acquired Limitation,**" which requires that circumvention be undertaken on a "lawfully acquired device or machine on which the computer program operates, or is undertaken on a computer, computer system, or computer network on which the computer program operates with the authorization of the owner or operator of such computer, computer system, or computer network"[10]
    b. The "**Any Laws Limitation**" which requires that researchers "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."[11]

[8] 37 C.F.R § 201.40(b)(11)(i) & (ii).

[9] 37 C.F.R § 201.40(b)(11)(ii).

[10] 37 C.F.R § 201.40(b)(11)(i).

[11] *Id.*

Removing this language, as well as related surplusage, would result in the following formulation:

> (i) Computer programs, where the circumvention is undertaken for the purpose of good-faith security research.
>
> (ii) For the purposes of this paragraph, "good-faith security research" means accessing a computer program for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in an environment designed to avoid any harm to individuals or the public.[12]

These changes accord with the 2018 recommendation of the National Telecommunications and Information Administration (NTIA) that the Office should "increase the clarity by removing requirements that overly complicate exemptions.[13] This proposed language also tracks NTIA's recommendation that exemption language should "only include exemption requirements that focus on protecting copyrighted works."[14]

NTIA also recommended that the Office adopt a "more structured" approach to applications for exemptions by laying out the "class of work, groups of beneficiaries, and types of circumvention permitted" to "improve readability" and streamline the process for managing applications for renewal or expansions during

---

[12] This would replace both subparagraph (i) and (ii) at 37 C.F.R 201.40(b)(11).

[13] 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.

[14] *Id.* To accord with this recommendation, the Office may also wish to consider whether to remove the limitation of the exemption to circumstances "where such activity is carried out in an environment designed to avoid any harm to individuals or the public." *See* 37 C.F.R. § 201.40(b)(11)(ii). We appreciate the Acting Register's 2018 refinement of this limitation's language and clarification that this limitation is not intended to micromanage specific aspects of a research environment—both helpful movements toward alleviating the chilling effects discussed during the previous triennial review. *See* Recommendation of the Acting Register of Copyrights at 307-08 (Oct. 2018) (2018 Recommendation), https://cdn.loc.gov/copyright/1201/2018/2018_Section_1201_Acting_Registers_Recommendation.pdf. However, the Acting Register drew no connection between this limitation and an interest in protecting against copyright infringement, *see* 2018 Recommendation at 307-08, and it is doubtful that it is wise policy or consistent with the limitations of Section 1201 or the Office's or the Library's authority to maintain the prohibition on circumvention as the appropriate context in which to address concerns about public safety.

each rulemaking.[15] Under this potential new framing of the exemptions, our proposed modifications would result in the following language:

Class: Computer programs

Use: Good-faith security research—accessing a computer program for the purposes of good-faith testing, and/or correction of a security flaw or vulnerability

Limit: The use is carried out in an environment designed to avoid any harm to individuals or the public;

[15] *Id*. at 4.

Item C. Overview

Our world continues to run on software. Software underlies nearly every aspect of modern life—from digital devices that we interact with on a daily—or even hourly—basis, to the public infrastructure that runs our everyday lives. Software underlies the World Wide Web, vehicles, home appliances, our elections, and our life-saving medical devices.

The ubiquity of software in modern life makes ensuring the security of digital devices essential to our personal security, national defense, and even the integrity of our democracy itself.[16] These threats aren't merely hypothetical, but real and persistent. Ransomware attacks have become increasingly common across a wide variety of industries, potentially exposing the private data of millions of consumers.[17] In the midst of the COVID-19 pandemic, hospitals have become an increasingly popular target for these kinds of attacks.[18] The pandemic has also created a new atmosphere of opportunity for malicious actors as more people are working from home and increasingly dependent on digital applications for everyday services.[19] The integrity of our elections is also at stake as states use digital solutions as part of their election infrastructure.[20]

While security research has become an increasingly important part of our modern cybersecurity architecture, an unclear legal landscape has continued to chill security researchers' ability to undertake efforts to protect our personal devices and critical infrastructure. The Digital Millennium Copyright Act (DMCA) is just one of a number of antiquated digital regulations that creates significant burdens for security researchers engaging in critical cybersecurity work.

---

[16] Adam Gorlick, *Obama at Stanford: Industry, government must cooperate on cybersecurity*, Stanford News (Feb. 13, 2015) https://news.stanford.edu/2015/02/13/summit-main-obama-021315/.

[17] Catalin Cimpanu, *Ransomware attacks accounted for 41% of all cyber insurance claims in H1 2020*, ZDNet (Sep. 10, 2020), https://www.zdnet.com/article/ransomware-accounts-to-41-of-all-cyber-insurance-claims/.

[18] Shannon Bond, Vanessa Romo, & Laurel Wamsley, *U.S. Hospitals Targeted In Rising Wave Of Ransomware Attacks, Federal Agencies Say*, NPR (Oct. 29, 2020) https://www.npr.org/2020/10/29/928979988/u-s-hospitals-targeted-in-rising-wave-of-ransomware-attacks-federal-agencies-say.

[19] INTERPOL, *INTERPOL report shows alarming rate of cyberattacks during COVID-19, Interpol* (Aug. 4, 2020), https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

[20] Jasime Webb, *Security Experts Say Online Voting Is a Bad Idea. Here's Why, Medium* (July 20, 2020) https://medium.com/digital-diplomacy/security-experts-say-online-voting-is-a-bad-idea-heres-why-1792c9a876b0.

The current temporary exemption to Section 1201 is flawed for two distinct but related reasons. Both of these limitations expand the analysis for exemptions beyond Section 1201's original purpose: to protect against infringement of digitally distributed copyrighted content.

Specifically, the Use Limitations leave uncertainty as to what sorts of post-circumvention conduct—such as engaging in criticism or scholarship—is encompassed within the definition of "good-faith security research." This ambiguity raises significant constitutional problems in light of the U.S. District Court's recent ruling in *Green v. Department of Justice*.[21] The *Green* court concluded that Section 1201 may create an "as-applied" restraint of the First Amendment rights of security researchers.[22]

Similarly, the Other Laws Limitations expand Section 1201 into a generalized tool for resolving questions of cybersecurity law and policy wholly unrelated to copyright law. These limitations allow firms to bring frivolous claims against security researchers by abusing the ambiguity in the current exemption to transform Section 1201 into a sword to deter unwanted criticism or scrutiny.[23]

While Section 1201 and the shortcomings in the exemption have continued to chill security research, other federal agencies and private actors have been actively working to encourage and facilitate security research. The Department of Defense and the State Department offer "bug bounty" programs that reward—rather than deter—valuable security research.[24] These kinds of incentives for security research have a long history of use in the private sector and have become an increasingly popular tool for major companies like Google and Apple to protect the security of

---

[21] 392 F.Supp.3d 68 (D.D.C. 2019)

[22] *Id.* at 94-96.

[23] See discussion of Voatz's efforts to deter criticism and the youtube-dl incident *infra*, Item E.3.i.

[24] *See U.S. Dept. of Defense Vulnerability Disclosure Policy*, hackerone, https://hackerone.com/deptofdefense?type=team (last visited Dec. 14, 2020); *see also* Catalin Cimpanu, *US offers $10 million reward for hackers meddling in US elections*, zdnet (Aug. 5, 2020) https://www.zdnet.com/article/us-offers-10-million-reward-for-hackers-meddling-in-us-elections/; Joseph Marks, *The Cybersecurity 202: DARPA wants hackers to try to crack its new generation of super-secure hardware*, Washington Post (Jun. 8, 2020), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/06/08/the-cybersecurity-202-darpa-wants-hackers-to-try-to-crack-its-new-generation-of-super-secure-hardware/5edd383d88e0fa32f82346f1/.

their networks.[25] This dynamic places the exemption increasingly at odds with national cybersecurity policy and best practices.

Many software and hardware companies increasingly welcome—and in some cases explicitly invite—security research, but some firms nevertheless remain unaccustomed to—and in many cases outright hostile towards—independent efforts to test the security of their systems. For example, companies like Voatz, a vendor of voting systems, have used ambiguities in various laws—which can be exploited under Section 1201 via the maintenance of the Any Laws Limitation—to threaten and intimidate researchers to prevent unwanted public scrutiny into vulnerabilities in their services.[26]

In response to incidents like this, Congress is actively considering modifications to Section 1201 in order to better promote security research.[27] In questions submitted for the record, numerous Senators sought input on whether the triennial rulemaking process itself creates untenable burdens for parties attempting to receive an exemption from anti-circumvention prohibitions,[28] and Senator Blumenthal specifically asked whether a more robust permanent exemption is necessary to facilitate security research into critical infrastructure such as election technologies.[29]

Security research is essential to the operation and security of our modern world. Good-faith disclosures of vulnerabilities by security researchers make complex technologies more transparent and help companies design safer products for the future.[30] In cases where firms are uninterested in—or outright hostile

---

[25] *See Google Vulnerability Reward Program Rules*, Google, https://www.google.com/about/appsecurity/reward-program/index.html (last visited Dec. 13, 2020); *see also* Oliver Haslam, *Apple is now supplying bug bounty hunters with special iPhones*, iMore (Jul. 22, 2020) https://www.imore.com/apple-now-supplying-bug-bounty-hunters-special-iphones.

[26] *See* Response to Voatz's Supreme Court Amicus Brief, disclose.io (Sep. 14, 2020) https://disclose.io/voatz-response-letter/.

[27] *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.

[28] *See id*.

[29] *Id*. at 13.

[30] *See* Joseph Lorenzo Hall, et al., *The Importance of Security Research* (Dec 2017), https://cdt.org/insights/the-importance-of-security-research-four-case-studies/; *see also* Edward Felten, *The Chilling Effects of the DMCA*, Slate Magazine, (Mar 29,

towards—vulnerability disclosures, security researchers should still be permitted to inform the public about critical safety flaws in essential technologies from smartphones to voting machines. Removing the limitations to the current temporary exemption and codifying a more robust, permanent exemption is necessary to facilitate critical security research. These changes would keep Section 1201 narrowly focused on copyright infringement and stop it from gradually expanding, contrary to Congress's intent, into a vehicle for resolving questions about security research policy wholly outside the Office's jurisdiction.

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

The record in previous triennial rulemakings has well established that TPMs are detrimental to good-faith security research.[31] As Prof. Halderman pointed out in the 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."[32] Prof. Halderman also observed that the Register has noted that "a significant number of product manufacturers employ TPMs on computer programs" and that "[p]roponents establish in the record that in many instances these TPMs have an adverse impact on the ability to engage in security research."[33] The Office's recommendation to grant the security research exemption in 2015 and renew it in 2018 and 2020 all indicate that TPMs have—and will continue to create—adverse effects on security research.[34]

As we have noted previously, nearly every product employs TPMs to discourage circumvention.[35] Common TPMs employed by software companies include challenge response measures (such as access codes, passwords, keys, digital signatures), encryption, and software designed to prevent tampering.[36] Of concern

---

2013), http://www.slate.com/articles/technology/future_tense/2013/03/dmca_chilling_effects_how_copyright_law_hurts_security_research.html.

[31] *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.

[32] *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).

[33] 2018 Comment at 7 (quoting 2015 Recommendation at 305)

[34] *See* 2015 Recommendation at 299; Section 1201 Rulemaking; 2018 Recommendation at 313; 2020 NPRM, 85 Fed. Reg. at 65,300-301.

[35] 2018 Comment at 7 (citations omitted).

[36] *Id.* at 6-8.

to security researchers are several classes of common protection measures—including measures controlling installation, execution, or use, measures controlling reading or inspection, and measures controlling modification, as well as general methods used to circumvent those measures.[37] These measures often must be circumvented in order to conduct research on a variety devices including voting machines.[38]

Item E. Asserted Adverse Effects on Noninfringing Uses

The NPRM encourages commenters to focus on the following elements to demonstrate that proposed modifications to existing exemptions satisfy the requirements for the exemption to be granted under Section 1201:

1. The proposed class includes at least some works protected by copyright;
2. The proposed uses are noninfringing under title 17;
3. Users are adversely affected in their ability to make such noninfringing uses and users are likely to be adversely affected in their ability to make such noninfringing uses during the next three years; and
4. The statutory prohibition on circumventing access controls is the cause of the adverse effects.[39]

The proposed modifications do not change the underlying class of works in the existing exemption, which the Acting Register concluded in 2018 includes at least some works protected by copyright.[40] The Register also concluded in 2015 that good-faith security research is a noninfringing use, and the intended uses that the modifications would enable do not differ in any way material to the question of infringement.[41]

Researchers are adversely affected in their ability to conduct such noninfringing research. The Use Limitations adversely affect noninfringing research by creating uncertainty around researchers' ability to use derived information to engage in constitutionally protected speech such as scholarship, teaching, and warning consumers about security flaws.[42] The Other Laws Limitations adversely affects noninfringing research by creating uncertainty through the introduction of extraneous legal regimes wholly unrelated to copyright.[43] In 2018, the Register concluded that the statutory prohibition on circumventing access controls is the cause of the adverse effects, and though the adverse effects of the current

---

[37] *Id.*

[38] *Id.*

[39] 2020 NPRM, 85 Fed. Reg. at 65,294, 65,301.

[40] *See* 2018 Recommendation at 290.

[41] 2015 Recommendation at 300.

[42] See discussion *infra*, Item A.3.i.

[43] See discussion *infra*, Item A.3.ii.

exemption are slightly different, the adverse effects are similarly directly caused by the prohibition on circumvention.[44]

1. The proposed class includes at least some works protected by copyright.

The Acting Register concluded in her 2018 Recommendation that the proposed class is defined to include computer programs, which are copyrightable works."[45] The Librarian incorporated this into the Final Rule by noting that the Register found that "legitimate security research has been hindered by TPMs that limit access to [copyrighted computer programs]."[46] The proposed modifications do not change the underlying exemption's coverage of computer programs, and thus also include at least some works that are protected by copyright.

2. The security research enabled by the proposed exemption is noninfringing.

In 2018, the Acting Register determined that good-faith security research was likely to be a non-infringing use[47]—a conclusion that the Register affirmed in announcing plans to renew the existing exemption.[48] Computer security research often is not concerned with access to the creative, expressive elements of computer software and is instead primarily concerned with functional elements unprotectable by copyright. Even if the underlying work is found to be copyright-protected, the security research will be fair use, just as the Acting Register determined that security research was fair use in 2018.[49]

i. Most computer security research does not implicate exclusive rights of copyright holders in underlying computer programs.

Computer security research typically involves accessing the functional aspects of the works not subject to copyright and thus does not constitute an infringing act. Protection established under the Copyright Act is limited to original works of authorship and "does not extend to the ideas underlying a work or to the functional or factual aspects of the work."[50] As Prof. Halderman explained in 2018 rulemaking, while software and devices subject to security research have both creative and functional elements, good-faith security research often focuses on the functional elements such as unprotectable elements of a computer program's object

---

[44] *See* 2018 Recommendation at 312-13.

[45] *Id.* at 290.

[46] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed Reg. 65,944, 65,956.

[47] 2018 Recommendation at 298.

[48] *See* 2020 NPRM, 85 Fed. Reg. at 65,300-301

[49] 2018 Recommendation at 298.

[50] Sega v. Accolade, 977 F.2d 1510 (9th Cir. 1992), as amended (Jan. 6, 1993) (citing 17 U.S.C. § 102(b)).

code.[51] Such functional elements are excluded from copyright protection. Moreover, the primary aim of security research is investigation, not reproduction, distribution or adaptation of copyrighted works.

The Acting Register agreed in 2018 that the computer programs at issue in the existing exemption are "likely to fall on the functional rather than creative end of the spectrum."[52] None of the proposed modifications lead to a different conclusion. The underlying works that researchers will access are largely functional in nature, mitigating any concerns about infringing authors' rights to the expressive elements of works.

ii. Even if computer security research does implicate copyright, it is a noninfringing fair use.

Even where security research involves more than *de minimis* reproduction, distribution, adaptation, or some other exclusive right, it is universally likely to be a non-infringing fair use under the familiar four-factor test:

1. the purpose and character of the use, including whether such use is for commercial or nonprofit, educational purposes;
2. the nature of the copyrighted work;
3. the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
4. the effect of the use upon the potential market for or value of the copyrighted work.[53]

In 2018, the Acting Register determined that good-faith security research was likely to be fair use,[54] a conclusion reaffirmed by the Register's plans to renew the existing exemption.[55] The uses proposed by this modification petition are the same as those uses proposed in 2018.

This fair use analysis relates to all the requested modifications because the current limitations restrict good-faith security researchers' noninfringing activities. Except where noted, the fair use factors apply in the same or substantially similar ways for each of the good-faith security research uses that would be permitted if the modifications to the existing exemption were granted.[56] While it is difficult to

---

[51] 2018 Comment at 11; *see, e.g.*, Sony v. Connectix, 203 F.3d 596, 602 (9th Cir. 2000) (citing 17 U.S.C. § 102(b)).

[52] 2018 Recommendation at 296 (quoting 2015 Recommendation at 301).

[53] *See* 17 U.S.C. § 107.

[54] 2018 Recommendation at 298.

[55] 2020 NPRM, 85 Fed. Reg. at 65,300-301

[56] Contrary to the Office's 2018 conclusion, retaining the Other Laws Limitation in the context of the fourth factor is not required in order to find that the underlying

offer a specific infringement analysis for each individual use, all of the uses are consistently under the banner of fair use and therefore support the modification of this exemption since they will not result in copyright infringement.[57] The proposed exemption does not seek to insulate activities that go beyond security research.

Purpose and character. The purpose and character of the proposed security research weighs in favor of fair use, as it did in 2018. In 2018, the Acting Register determined the first factor weighted in favor of fair use, finding that "many of the activities involved in security research are likely to be transformative, as the copying and alteration of the programs are for the purpose of providing information about those works—their susceptibility to security breaches—and do not 'merely "supersede[] the objects' of the original creation."[58]

None of the proposed modifications to the current exemption would materially affect the first factor analysis provided by the Acting Register during the last rulemaking. Removal of the Other Laws Limitations, for example, would merely eliminate the uncertainty imported from laws such as the Computer Fraud and Abuse Act and other legal regimes wholly unrelated to copyright.

Removal of the Use Limitations likewise would not have a significant impact on the purpose and character of the proposed uses. During the last rulemaking, the Acting Register rejected concerns that an expanded exemption without the Use Limitations would "apply to a broader range of uses, including commercial activities, that may not be transformative."[59]

The additional proposed activities are once again of the same purpose and character; removal of the Use Limitations would merely ensure that security researchers would not be chilled as they engage in scientific dialogue, classroom teaching and other scholarship, activities long established in Section 107 to be transformative in nature. Thus, the first factor weighs heavily in favor of fair use, and each limitation should be removed because they restrict noninfringing uses.

Nature of the works. The nature of the works factor again militates toward fair use. In 2018, the Acting Register found that the intended use cases for security research are "focused on programs used to operate machines, devices, or systems"

---

market is not affected by security research. *Contra* 2018 Recommendation at 298. See discussion *infra*, Part E.2.ii (effect on the relevant market).

[57] *See* 17 U.S.C. § 1201(a)(1)(C).

[58] 2018 Recommendation at 294 (quoting Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 579 (1994)); *see also* 2020 NPRM, 85 Fed. Reg. at 65,300-301 (implicitly endorsing the same analysis).

[59] *See* 2018 Recommendation at 292-94, (quoting Auto Alliance Class 10 Opposition at 4). "[T]he fact that the disputed use of copyrighted material is commercial is not determinative in and of itself." A.V. ex rel. Vanderhye v. iParadigms, 562 F.3d 630, 639 (4th Cir. 2009).

and thus "are likely to fall on the functional rather than creative end of the spectrum."[60]

The intended use cases for the current expansion petition are again as they were in 2018. The Use Limitations do not expand the realm of underlying programs subject to research. Likewise, removing the Other Laws Limitations would only affect the requirement that the circumvention is undertaken on a lawfully acquired device and would not change the type or character of program subject to research. Thus, this factor continues to weigh in favor of fair use.

Amount and substantiality. The third factor looks at the amount and substantiality of the portion used in relation to the copyrighted work as a whole. In 2018, the Acting Register found "this factor to be of little significance" in the context of security research.[61] The Acting Register noted that "courts have been willing to permit complete copying of the original work . . .where it is necessary to accomplish a transformative purpose," further noting that the third factor is "not accorded significant weight were functional elements of a program cannot be investigated without some intermediate reproduction."[62]

The analysis under this factor is again the same as it was in 2018. Here, neither the modifications to the Use Limitations or the Other Laws Limitations would substantially change the amount of the copyrighted work being used. As mentioned in 2018, copying of protected elements is sometimes necessary to adequately investigate security concerns, but any copying is merely incidental to the actual goal of the research.[63] Publication of security research rarely contains any substantial portions of the original work.[64]

Effect on the relevant market. The fourth factor has long been considered the most important factors in the fair use assessment.[65] In 2018, the Acting Register found that the fourth factor weighed in favor of fair use, concluding that speculative market concerns are unavailing and noting that customers being "scare[d] . . . away from" software providers due to vulnerabilities being exposed is

---

[60] 2018 Recommendation at 295-296, *see also* 2020 NPRM, 85 Fed. Reg. at 65,300-301 (implicitly endorsing the same analysis).

[61] 2018 Recommendation at 296 (citing 2015 Recommendation at 301).

[62] *Id.* (internal citations omitted).

[63] 2018 Comment at 16.

[64] *Id.*

[65] *See* Harper & Row v. Nation, 471 U.S. 539, 566 (1985) ("Th[e fourth] factor is undoubtedly the single most important element of fair use.").

"precisely the type of reputational harm that the courts have held non-cognizable under the fourth factor."[66]

The Acting Register wrongly concluded in 2018 that this finding is at least partially contingent on the continued presence of the Lawfully Acquired Limitations, noting that acquisition of devices in violation of the law "plainly is conduct that, were it to become widespread, would adversely affect the software copyright owner's potential market."[67] The purpose of the market factor analysis is to protect real markets cognizable under copyright, not to protect every conceivable market from all conceivable harm under all legal regimes. When acquiring a device on which copyrighted software is installed, consistency with other non-copyright law is not a relevant consideration toward whether security research on the software is infringing.

Moreover, the norms and standards among the research community demonstrate that researchers have no intention of flouting the law in acquiring devices. However, the record is replete with examples of researchers obtaining devices through legal means and later being threatened with liability for violations of unknown agreements with third parties.[68] Thus, the Office should not rely on the "lawfully obtained" language to determine this factor favors fair use.

3. Section 1201 continues to impose adverse effects on researchers performing noninfringing security research and likely will continue to do so over the next three years.

The Register concluded in 2015 that TPMs protecting computer programs have a "substantial adverse impact on good-faith testing for and the identification, disclosure and correction of malfunction, security flaws and vulnerabilities in the protected computer program"[69]—a conclusion underscored by the Office's recommendations to renew the exemption in 2018[70] and 2020.[71] The Register also concluded in 2015 that Section 1201's built-in exemptions are insufficient to protect the interests of security researchers:

> The Register therefore concludes that, based on the current record, the permanent exemptions embodied in sections

---

[66] 2018 Recommendation at 298 (quoting Election System Providers Class 10 Opposition at 20) (citing 2015 Recommendation at 302 (internal citations omitted); *see also* 2020 NPRM, 85 Fed. Reg. at 65,300-301 (implicitly endorsing the same analysis).

[67] 2018 Recommendation at 298.

[68] See discussion *infra*, Item F.1 (Documentary Statement of Harri Hursti and J. Alex Halderman).

[69] 2015 Recommendation at 305.

[70] 2018 Recommendation at 313.

[71] 2020 NPRM, 85 Fed. Reg. at 65,300-301

> 1201(j), 1201(f) and 1201(g) do not appear unambiguously to permit the full range of legitimate security research that could be encompassed by the proposed exemption. In light of this uncertainty, the Register proceeds to consider an exemption for the proposed uses.[72]

The Register also noted that a "significant number of product manufacturers employ TPMs on computer programs," and that "in many instances these TPMs have an adverse impact on the ability to engage in security research."[73] The Register conceded that "significant independent research is taking place through the cooperation of copyright owners," but emphasized that "despite the existence of authorized research," adverse effects persist.[74]

Despite the clear recognition by the Register that: (1) TPMs have substantial adverse effects on noninfringing security research and (2) the existing exemptions are insufficient to allow for the full range of legitimate security research, the Office has failed to take the necessary actions to remedy the problem and eliminate the ambiguities under the current regime. While the record in this—and past—proceedings are replete with examples of the significant adverse effects on non-infringing security research, new evidence highlights how both the Use and Other Laws Limitations are the primary source of these effects.

i. The Use Limitations chill the ability of security researchers to engage in constitutionally protected speech.

The Use Limitations make it unclear what sorts of post-circumvention conduct—such as engaging in criticism or scholarship—the definition of "good-faith security research" encompasses. Uncertainty concerning the scope and definition of the "solely" requirements within the Purpose Limitation deprives researchers of sufficient clarity about whether the exemption permits engaging in scholarship or criticism related to copyrighted materials protected by a TPM. Likewise, the Security Limitation requires that information be used "primarily" to improve the security of devices, adding confusion to researchers' ability to engage in valuable public discourse concerning cybersecurity policy that isn't *per se* tied to improving the security of specific devices.

The Purpose Limitation. Ambiguity concerning the definition of "solely" in the Purpose Limitation allows for malicious litigation against security researchers who—in addition to disclosing the results of their research to software developers—also attempt to inform the public about dangerous vulnerabilities in software.

---

[72] 2015 Recommendation at 309.

[73] *Id.* at 305.

[74] *Id.* at 305-306.

One example of a security researcher who has faced this problem is Dr. Matthew Green.[75] Dr. Green has been subject to threats of litigation from developers that seek to use Section 1201 as a sword to deter unwanted criticism or scrutiny, rather than its intended purpose as a mechanism for protecting copyright holders.[76] Because of past experiences with frivolous litigation, Dr. Green and his co-plaintiffs filed a pre-enforcement challenge seeking relief from both criminal prosecution and civil liability for circumventing TPMs.[77]

In response to the government defendants' motion to dismiss, the District Court for the District of Columbia concluded that Section 1201 may create an "as-applied" restraint of Dr. Green's First Amendment rights.[78] Applying intermediate scrutiny, the *Green* court found that Dr. Green and his co-plaintiffs had made a compelling case that the defendants had failed to meet their burden to demonstrate that Section 1201 did not burden substantially more speech than necessary.[79]

While both parties agreed that Section 1201 was enacted pursuant to a legitimate government interest: stopping infringement of copyrighted materials,[80] the court agreed with Dr. Green that Section 1201 was not tailored to that interest.[81] The court credited Dr. Green's argument that Section 1201 burdens more speech than necessary because there is no market for the kinds of software for which Dr. Green and his co-plaintiffs sought to circumvent TPMs, let alone software tools designed to circumvent those TPMs.[82]

The kinds of software on which Prof. Halderman and many other security researchers seek to circumvent TPMs similarly lacks a cognizable market that needs protection from online infringement. For example, voting machines are purchased as a turn-key service that includes both hardware elements and software designed to run on those systems.[83] Prof. Halderman and other researchers seek to

---

[75] Dr. Green has previously participated in the Triennial Rulemaking Process seeking an expanded security research exemption. *See generally* Initial Comments of Matthew Green Regarding Class 10, Docket No. 2017-10 (Dec. 18, 2017) https://cdn.loc.gov/copyright/1201/2018/comments-121817/class10/class-10-initialcomments-green.pdf.

[76] *Green*, 392 F.Supp.3d at 78-79.

[77] *Id*.

[78] *Id*. at 94-96.

[79] *See id*. at 96 (quoting Turner v. FCC, 512 U.S. 622, 665 (1994)).

[80] *Id*. at 94.

[81] *See id*. at 95.

[82] *Id*. (quoting Pls' Opp'n, ECF No. 18 at 43, *available at* https://copyrightalliance.org/wp-content/uploads/2016/10/EFF-DOJ.pdf).

[83] See discussion *infra*, Item F.1 (Documentary Statement of Harri Hursti and J. Alex Halderman).

circumvent TPMs on these systems to audit software for potential vulnerabilities.[84] After conducting this kind research, Prof Halderman and other researchers simply seek to publish code snippets in their research to highlight and discuss the vulnerabilities they have identified—not to reuse, resell, or otherwise repurpose the software. Even if the publication had some impact on the potential market—such as by dissuading election administrators from purchasing services from vendors that produce vulnerable election software—that would not be the kind of market effect protectable by copyright law.[85]

Given the constitutional dragons lurking around the application of Section 1201 to security research, the Office must broaden the exemption to be as permissive as possible. Doing so is the only way to reconcile Section 1201's operation with the First Amendment.

Rather than providing clear guidance to security researchers on how language will be interpreted and understood when considering the applicability of exemptions, the Office has, in the past, doubled down on ambiguities created by Congress. In 2015, the Register did not give any specific justification for including the word "solely." Rather, she reasoned that "in the interest of adhering to Congress's basic purpose in Section 1201(j), where appropriate, the recommended exemption tracks Congress's language rather than the alternative formulations suggested by proponents."[86] Indeed, the usage of "solely" in the Purpose Limitation tracks exactly with the use of "solely" in §1201(j).[87] Since 2015, the Register has not issued any significant additional guidance on how "solely" should be interpreted.[88]

We urge the Office to reverse course here. Simply tracking Congress's wording across exemptions is not sufficient to justify the adverse effects that this limitation has on security research. This approach is even more concerning given the as-applied restraint of speech noted by the *Green* court. In drafting the DMCA—and Section 1201 in particular—Congress failed to sufficiently tailor the language to avoid an unconstitutional restraint on free speech. Importing this same language into the temporary and permanent exemptions simply perpetuates the statute's constitutional infirmities.

Moreover, Congress has recognized that the Office's current approach to Section 1201 creates untenable problems for security researchers. During a recent hearing convened to explore reforms to Section 1201, numerous Senators sought input on whether the triennial rulemaking process itself creates untenable burdens

---

[84] *See id.*

[85] *See Harper & Row*, 471 U.S. at 568-569 (limiting the scope of cognizable market effects to direct competition with a copyright holder's original work).

[86] 2015 Recommendation at 319.

[87] *See* 17 U.S.C. § 1201(j).

[88] *See* 2018 Recommendation at 305-06.

for parties attempting to receive an exemption from anti-circumvention prohibitions,[89] and Senator Blumenthal specifically asked whether a more robust permanent exemption is necessary to facilitate security research into critical infrastructure such as election technologies.[90]

Removing the term "solely" from the exemption limitations to a circumvention performed "for the purpose of good-faith security research" would clarify that researchers can circumvent TPMs in furtherance of scientific dialogue, academic peer review, and classroom teaching. The current exemption does not clarify whether these kinds of post-circumvention conduct—which qualify as both free expression and valid fair uses—are allowed. This ambiguity chills research and the resulting comments or reporting because researchers are hesitant to open themselves up to the possibility of litigation and may thus be more circumspect in discussing their research in the press or wary of publishing their results in academic journals. Removing this ambiguous language would ensure that the security research exemption is narrowly tailored to the purpose for which it was enacted—protecting the rights of copyright holders against infringement—and also afford proper breathing room for the First Amendment rights of security researchers.

The Security Limitation. The Security Limitation is similarly ambiguous particularly in the context of the word "primarily." A narrow reading might interpret "primarily" to mean "only"—excluding conduct like engaging in scholarship which does not directly improve the security of devices, but rather contributes to scientific discussion. For example, a researcher might feel after conducting a security audit that in addition to disclosing the vulnerability to the software developer, the public should also be warned about the potential security risks. While this *could* be interpreted as improving security for "those who use" the device, the Office has not provided sufficient clarity around how this limitation will be interpreted.

The Security Limitation is subject to the same constitutional issues discussed in the proceeding section with regards to the *Green* case. Two recent examples drive home the problems created by both of the Use Limitations with regard to the uncertainty faced by security researchers. Both of these incidents involve litigation—or threats thereof—faced by security researchers from entities attempting to use Section 1201 outside the scope of its intended purpose to provide an extra layer of protection against infringement. Removing the ambiguous language in both of these limitations would provide sufficient clarity for security researchers to engage in their important work without the fear of copyright liability or malicious litigation.

The Use Limitations are especially concerning in light of efforts by some vendors to intimidate researchers who attempt to warn the public against using

---

[89] *See* Reid 2020 QFR Response, *supra* note 27.

[90] *Id*. at 13.

services with critical vulnerabilities. For example, Voatz—a "blockchain" voting company—routinely uses ambiguities in cybersecurity laws and regulations to dissuade researchers from criticizing their platform.[91] All of the researchers targeted by Voatz sought to comply with the firm's disclosure policy, conducted research within the bounds of the CFAA, and the temporary security research exemption to the DMCA.[92] Nevertheless, Voatz threatened litigation when they realized that publication of research would negatively impact their business because researchers had identified intractable critical vulnerabilities.[93] Bad actors like Voatz could pursue litigation against researchers simply for attempting to warn the public against using their platform on the theory that this kind of criticism is not "primarily" related to improving the security of devices.

In another incident, the Recording Industry Association of America (RIAA) recently filed a malicious takedown notice against GitHub[94] related to a project hosted on their website.[95] The project in question, youtube-dl, is a tool that allows users to download videos from the popular website YouTube.[96] The RIAA filed a notice-and-takedown request under Section 512 of the DMCA, claiming that youtube-dl violated Section 1201 because it allowed for circumvention of a TPM.[97] After consulting legal counsel, GitHub eventually republished youtube-dl on their website.[98]

While the youtube-dl incident did not involve security research, it illustrates the potential threats faced by security researchers. Security researchers regularly use GitHub and platforms like it to host and share their work.[99] Without additional clarification from this Office, copyright holders are likely to follow the RIAA's example to intimidate developers and security researchers into removing content, using the vagaries of the exemption as a basis to pursue meritless takedowns. For example, a company like Voatz might file a notice-and-takedown claim against a

---

[91] Response to Voatz's Supreme Court Amicus Brief, *supra* note 26.

[92] *Id*.

[93] *Id*.

[94] GitHub is a distributed version control system for software development. *See* Arnaud Sahuguet, *GitHub: the Swiss army knife of civic innovation?*, Medium (Mar. 25, 2015) https://medium.com/@sahuguet/github-the-swiss-army-knife-of-civic-innovation-d2ba67288abb.

[95] Abby Vollmer, Standing Up for Developers, The GitHub Blog (Nov. 16, 2020) https://github.blog/2020-11-16-standing-up-for-developers-youtube-dl-is-back/

[96] *Id*.

[97] *Id*.

[98] *Id*.

[99] *See generally* GitHub Security Lab, https://securitylab.github.com/ (last visited Dec. 14, 2020).

security researcher for publishing work on GitHub that contains code snippets as well as a description of the circumvention methods used.

To better facilitate security research, the Office should remove both of the Purpose Limitations to ensure that researchers can continue their work without the potential threat of malicious litigation. Without these changes, researchers may be circumspect in discussing their work or reluctant to inform the public about critical vulnerabilities in applications from social media to election infrastructure. Even if the suits filed against researchers are entirely meritless, just the threat of litigation from a well-funded firm can be enough to dissuade security researchers—who often work for universities and non-profit organizations. Ultimately, removing the Purpose Limitations is necessary to ensure that Section 1201 is narrowly tailored to its original purpose of preventing infringement. Our requested changes will prevent Section 1201 from expanding into an omnibus tool to shield developers from unwanted criticism or silencing content that is an otherwise valid fair use.

ii. The Other Laws Limitations create uncertainty by tying the applicability of an exemption to non-copyright legal regimes

The Other Laws Limitations position Section 1201 as a potential cause of action against security research that is otherwise consistent with the existing exemption but entails a technical or minor violation of another law. Plaintiffs could bring claims under Section 1201 and 1203 based on technical infractions of laws such as the CFAA for which even the Department of Justice or other prosecuting entities have publicly committed not to pursue enforcement because of problems or ambiguities with the scope of that law.

The Lawfully Acquired Limitation requires that circumvention be undertaken on a "lawfully acquired device."[100] In cases where researchers acquire a device in a legitimate manner, they nevertheless cannot be certain whether they will still qualify for the exemption because the legality of acquisition is often dependent on the actions of third parties over which researchers have no knowledge or control.

The Any Law Limitation creates similar uncertainty by making the entire body of federal, state, and local law a trigger for liability under Section 1201. This is especially problematic in the context of laws like the CFAA that depend on nuanced prosecutorial discretion and guidance to differentiate purely technical violations that are rarely—if ever—litigated from instances where researchers are actually likely to face liability or prosecution.[101]

---

[100] 37 C.F.R § 201.40(b)(11)(i).

[101] Guidance from the DOJ states that "if [a] defendant exceeded authorized access [under the CFAA] solely by violating an access restriction contained in a contractual agreement or term of service with an Internet service provider or website, federal prosecution may not be warranted." *See* Department of Justice, Justice Manual Title 9-48000—Computer Fraud and Abuse Act (DOJ Manual),

The Other Laws Limitations, like the Purpose Limitations, unnecessarily expand the scope of Section 1201 outside of its narrow purpose to prevent infringement and into a vehicle for litigating issues of cybersecurity policy better left to—and in many cases explicitly delegated to—other agencies or state actors.

The Lawfully Acquired Limitation. This limitation creates significant uncertainty for security researchers concerning their potential liability, even where devices are obtained in an entirely legitimate manner. For example, the vendors of some classes of devices that researchers want to study, such as voting machines, place restrictions on buyers selling to third parties like researchers.[102] Because researchers often cannot purchase devices like these directly from the manufacturer or vendor, they must purchase these devices from third parties.[103] When purchasing devices such as a voting machine, security researchers cannot know for sure whether the seller had placed such a resale constraint on the original buyer.[104] This effectively conditions a researcher's ability to invoke an exemption on the existence of a contractual restraint of which the researcher may be entirely unaware. Additionally, liability for researchers in this case would be entirely dependent on the actions of a third party—specifically, the original seller's alleged violation of a contractual restraint—over whom researchers have no control.

Contractual restraints against resale are a creature of state law, creating even more confusion and uncertainty for security researchers. A researcher's potential for liability may depend on contract law within a specific state, leading to different outcomes depending on what state the security researcher resides in, what state the device was initially sold in, or the state in which the vendor operates or is incorporated in. This uncertainty makes it difficult for researchers to seek pre-research clearance from their counsel.

Moreover, in many cases, these contractual restraints against resale are placed on devices by manufacturers or vendors expressly for the purpose of deterring security research.[105] Security researchers might successfully avoid litigation or liability under contract law for violating these contractual restraints because of their lack of knowledge, but their unknowing violation of these restraints might preclude them from claiming an otherwise valid exemption to Section 1201.

Any Law Limitation. While the Lawfully Acquired Limitation creates uncertainty for security researchers based on the applicability of state contract law, the Any Law Limitation implicates these issues as well as other complex questions

---

https://www.justice.gov/jm/jm-9-48000-computer-fraud (last visited Dec. 13, 2020).

[102] See discussion *infra*, Item F.1 (Documentary Statement of Harri Hursti and J. Alex Halderman).

[103] *Id.*

[104] *Id.*

[105] *Id.*

of law under *any law* in the entirety of the US Code, state law, and county or municipal regulations.

Security researchers usually work for universities or other non-profit institutions, and thus cannot afford to hire sophisticated legal counsel that is qualified to opine on the applicability of various legal regimes including—but not limited to—the DMCA, the CFAA, the Wiretap Act, various federal and state level privacy laws, and every state's contract law.[106] It can be difficult for security researchers to engage and afford an attorney to give them qualified advice on even one of these legal regimes.

Because of the Any Laws Limitation, security researchers seeking to circumvent TPMs must find legal counsel that can opine on the interactions of *all* of these legal regimes. This usually leaves security researchers dependent on a small number of specialized technology law clinics to provide advice. While clinics regularly offer assistance to security researchers, the demand far exceeds the supply of available legal help. This imbalance is so severe that the Harvard Cyberlaw Clinic recently published a guide aimed at helping security researchers and their lawyers navigate the unfamiliar legal pitfalls of conducting security research.[107]

For lawyers attempting to advise security researchers, it can be difficult to provide sufficient certainty concerning the applicability of the various legal regimes frequently implicated in security research. Advising clients on Section 1201 can be particularly problematic, because in addition to possessing the relevant knowledge of copyright law, lawyers will also need to consider the application of a wide range of other legal regimes—such as the CFAA—when considering whether or not a researcher can invoke an exemption to Section 1201.

Importing various legal regimes into the analysis for invoking an exception to Section 1201 is problematic for three main reasons:

1. Laws like the CFAA are enforced through nuanced prosecutorial discretion in order to distinguish between *technical* violations that are generally allowed and *malicious* violations that are usually prosecuted.[108] Relatedly, the text of the CFAA is ambiguous, leading to a current circuit-split concerning the appropriate standard to apply for evaluating those cases that actually are prosecuted by authorities.[109]

---

[106] *Id*.

[107] Sunoo Park and Kendra Albert, *Cyberlaw Clinic and EFF publish Guide to Legal Risks of Security Research* (Oct 30, 2020) https://clinic.cyber.harvard.edu/2020/10/30/cyberlaw-clinic-and-eff-publish-guide-to-legal-risks-of-security-research/.

[108] DOJ Manual, *supra* note 101.

[109] Brief of Amicus Curiae Electronic Frontier Foundation, Center for Democracy & Technology, and New America's Open Technology Institute in Support of Petitioner

2. Importing extraneous legal regimes into the analysis for an exemption to 1201 positions the Office to effectively rule on the contours of non-copyright laws that lay entirely outside the ambit of the Office's limited delegated authority. Even if the Office does not per se issue substantive rules on these extra-jurisdictional areas of law, the Office must consider the implications and applications of the conditions it includes in temporary exemptions to avoid inadvertently extending the reach of Section 1201 beyond the heartland of copyright considerations or exercising substantive judgment on areas of law outside its area of expertise or authority.[110]
3. Third, hanging the potential for liability under Section 1201 on extraneous legal regimes, in conjunction with 17 U.S.C. § 1203, creates a new cause of action for actors like Voatz or the RIAA to sue security researchers based on claims that have no actual basis in copyright law, but merely seek to leverage Section 1201 to intimidate critics or opponents.

The CFAA is particularly problematic in this context because it is an unusually broad statute that prohibits accessing a "protected computer" either "without authorization" or "in excess" of authorized access.[111] Because the statute's definitions are unclear, it is up to courts and prosecutors to define the boundaries of permissible conduct under the CFAA. To address the overbreadth concerns of security researchers, the Department of Justice has had to publish extra-statutory guidelines detailing how the Department approaches potential violations of the CFAA that fall within the scope of the statute's uncertainty.[112]

Even if this extra-statutory guidance from DOJ gives researchers confidence that they have taken the necessary steps to eliminate their potential for liability under the CFAA, the Any Laws Limitation nevertheless creates a basis for copyrighted holders to use technical, non-prosecuted violations of the CFAA as a basis for a claim under Section 1201. The text of the exemption explicitly references the CFAA but does not distinguish between the kinds of technical violations that are rarely—if ever—prosecuted, and violations premised on

---

at 3, Van Buren v. U.S., No. 19-783 (EFF Amicus Brief), https://www.eff.org/document/amicus-brief-van-buren-v-united-states. *See generally* Congressional Research Service, *From Clickwrap to RAP Sheet: Criminal Liability under the Computer Fraud and Abuse Act for Terms of Service Violations* (updated Apr. 27, 2020), https://crsreports.congress.gov/product/pdf/LSB/LSB10423.

[110] NTIA has urged the Office to reign in requirements in exemptions to Section 1201 that require it to "develop expertise in every area of policy that participants may cite to on the record" and "not deviate too far afield from copyright policy concerns." *See* 2018 NTIA Recommendation, *supra* note 13 at 2.

[111] 18 U.S.C. § 1030(a)(1).

[112] *See generally* DOJ Manual, *supra* note 101.

malicious conduct undertaken for purposes other than good-faith security research.[113]

Thus, researchers might still fail to qualify for an exemption to Section 1201 where they have committed a purely technical violation of the CFAA that is within the bounds of permissible research according to the DOJ. This could allow bad actors to use Section 1201 to pursue litigation against a security researcher in cases where a researcher has conducted their work within the bounds of the DOJ's security research guidance, and also hasn't actually facilitated any kind of copyright infringement.

Tying the temporary security research exemption to the CFAA is also problematic because of the current federal circuit split over the scope of the law's prohibition against unauthorized access.[114] One side of the circuit split hinges the analysis of whether the alleged violator has complied with the policies articulated by the owner of the targeted "computer."[115] Under this approach, a security researcher could be held liable simply for attempting to use a website in a manner that is inconsistent with that website's terms of services.[116] The other side of the circuit split tracks Congress' initial intent in passing the CFAA by considering whether an alleged hacker has actually *broken* into the computer *with malicious intent*.[117] Until the Supreme Court clarifies this circuit split, the ability of security researchers to invoke an exemption to Section 1201 will effectively depend on *where* the circumvention takes place or where the "protected computer" is located.

But even if these inconsistencies in the CFAA were eliminated, there are still fundamental issues related to tying exemptions granted under Section 1201 to extraneous legal regimes that govern cybersecurity policy or other areas of law. Conditioning the applicability of exemptions to Section 1201 on non-copyright legal regimes is problematic because of the limited scope of the Office's authority and expertise.

---

[113] *See* 37 C.F.R. § 201.40(b)(11)(i)

[114] The Second, Fourth, and Ninth Circuits interpret the statute's phrase "exceeding authorized access" narrowly, limiting it to instances of traditional hacking activity, U.S. v. Valle, 807 F.3d 508 (2d Cir. 2015); WEC Carolina Energy Solutions v. Miller, 687 F.3d 199 (4th Cir. 2012); U.S. v. Nosal, 676 F.3d 854 (9th Cir. 2012), while the First, Fifth, Seventh, and Eleventh Circuits read the phrase more broadly, including using a computer for purposes prohibited in a terms of use agreement, EF Cultural Travel BV v. Explorica Inc., 274 F.3d 577 (1st Cir. 2001); U.S. v. John, 597 F.3d 263 (5th Cir. 2010); Int'l Airport Ctrs. LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006); U.S. v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010)).

[115] EFF Amicus Brief, *supra* note 109 at 4.

[116] *Id.*

[117] *Id.*

More specifically, the Copyright Office derives its authority from Congress according to the Progress Clause, which allows for the promotion of "the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries."[118] Congress has made no effort to connect the other laws implicated here with the Progress Clause; for example, Congress appears to have relied upon the Interstate Commerce Clause, not the Progress clause, in enacting the CFAA.[119] Conversely, it is implausible that Congress could stretch the bounds of serving the progress of science and the useful arts to the point of using copyright law to reinforce general purpose computer hacking or surveillance laws—much less the broad ambit of *every other law* that the Other Laws Limitations sweep into Section 1201.

Moreover, Section 1201—and the DMCA at large—were enacted pursuant to an even *narrower* purpose: preventing copyright infringement.[120] Given the constitutional concerns discussed in the previous section, placing additional restraints on security research that are wholly unrelated to this narrow purpose only further undermines the government's argument that Section 1201 is narrowly-tailored enough to survive strict scrutiny.[121]

Even if determining the applicability of non-copyright laws does not unconstitutionally expand the Office's jurisdiction outside of its narrow mandate to protect copyright, answering these complex questions of law is beyond the scope of the Office's expertise. Indeed, agencies like the Department of Justice have intervened in previous rulemakings to admonish the Office for placing unnecessary restrictions on security research.[122] During the 2018 rulemaking, NTIA also urged

---

[118] U.S. Const. art. I, § 8, cl. 8

[119] For example, the text of Section 1030(e)(2)(B) defines a "protected computer" for the purpose of the CFAA as a computer which, "is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B) These constructions are standard formulations for any law passed pursuant to Congress' authority under the Commerce Clause. *See, e.g.*, Heart of Atlanta Motel v. U.S., 379 U.S. 241, 247, 256-258 (1964) (holding that similar language in the Civil Rights Act of 1964 was within Congress's authority under the Commerce Clause).

[120] *See generally* U.S. Copyright Office, *The Digital Millennium Copyright Act of 1998* at 4 (Dec. 1998), https://www.copyright.gov/legislation/dmca.pdf.

[121] See discussion *supra*, Item E.3.i.

[122] *See* Comments of DOJ Computer Crime and Intellectual Property Section, Docket No. 2017-10 (Jun. 28, 2018), https://www.justice.gov/criminal-ccips/page/file/1075496/download.

the Office to "not deviate too far afield from copyright policy concerns" in tailoring the exemption language.[123]

Finally, placing hooks into extraneous legal regimes makes Section 1201 even broader as a potential cause of action for firms seeking to intimidate critics or opponents. Copyright holders could use Section 1201 as a vehicle to bring claims against security researchers that likely would have been meritless under another body of law. Section 1201 is already prone to abuse because many courts treat it as lacking any requirement of a nexus to copyright infringement;[124] it need not be further removed from legitimate copyright interests by conditioning exemptions on "any other applicable law." Removing the extraneous legal hooks in the Other Laws Limitations will prevent firms from bringing these kinds of intimidation suits against security researchers in the future.

To be clear, removing the Other Laws Limitations will not shield security researchers from liability for intentional and malicious violations of laws such as the CFAA and the Electronic Communications Privacy Act (ECPA), but will provide significant clarity for researchers engaging in good-faith efforts to identify and disclose software vulnerabilities. Researchers who run afoul of the prosecutorial guidelines for laws like the CFAA will remain subject to prosecution by the agencies responsible for enforcing those laws or litigation from plaintiffs seeking to vindicate the legitimate infringement of a statutory right. But removing these limitations will make it easier for researchers—or their counsel—to understand and mitigate their legal risk under the Copyright Act. Removing the Other Laws Limitations will also make it simpler for the Office to assess the applicability of an exemption by removing the hooks to extraneous legal regimes wholly unrelated to copyright.

4. Section 1201's statutory factors cut in favor of granting the proposed modifications.

Under Section 1201(a)(1)(C), the Librarian of Congress considers five factors in whether to grant an exemption:

i. The availability for use of copyrighted works;

ii. The availability for use of works for nonprofit archival, preservation, and educational purposes;

iii. The impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;

iv. The effect of circumvention of technological measures on the market for or value of copyrighted works; and

[123] NTIA 2018 Recommendation, *supra* note 13 at 2.

[124] *See generally* Reid 2020 QFR Response, *supra* note 27.

v. Such other factors as the Librarian considers appropriate.[125]

In determining the weight of each factor in 2018, the Register found that the analysis for the first four factors was substantially the same as that in 2015 and that all factors were favorable towards the exemption.[126] In 2018, the Acting Register determined that there were no other major concerns to include in the fifth factor that would weigh against or in favor of granting the exemption.[127]

All statutory factors again weigh in favor of granting the exemption; the Office should particularly weigh the fifth factor in favor of the proposed modifications in light of the national cybersecurity policy priorities negatively affected by the existing exemption's narrow formulation.

i. Granting the exemption will increase the availability of copyrighted works that are aimed at rectifying security flaws.

In 2018, the Acting Register found that the first statutory factor favored a wider good-faith security research exemption.[128] The Acting Register stated that "granting the exemption would increase the availability of copyrighted works in the form of articles, presentations, and computer programs aimed at rectifying security flaws."[129] Further, in 2015, the Register reasoned that the "salient consideration" in this factor is "whether there will be greater availability of copyrighted works in general if an exemption is granted," and found that a negative impact on the availability of copyright works had not been established.[130]

Moreover, the exemption as currently scoped *negatively* impacts the availability of copyrighted works by chilling the publication of works by security researchers.[131] A good-faith security research exemption without limitations will increase the number of copyrighted works available for study. As security researchers are simply analyzing existing products for serious security flaws, this activity does not remove copyrighted information from the market or stifle copyrighted material from entering the market.

By contrast, removing both the Other Laws and Use limitations will result in more independent security research, and as a result, new and existing companies will likely bring new, more secure products to the market while additional copyrighted material will enter the market as security researchers publish their

---

[125] 17 U.S.C. § 1201(a)(1)(C).

[126] 2018 Recommendation at 312; *see also* 2020 NPRM, 85 Fed. Reg. at 65,300-301 (implicitly endorsing the same analysis).

[127] 2018 Recommendation at 312; *see also* 2020 NPRM, 85 Fed. Reg. at 65,300-301 (implicitly endorsing the same analysis).

[128] *Id.*

[129] *Id.*

[130] 2015 Recommendation at 310.

[131] See discussion *supra*, Item E.3.i.

findings. These activities likely will increase the availability of copyrighted material to the public, furthering a major copyright goal. Thus, this factor weighs in favor of granting the proposed modifications.

ii. Granting the proposed exemption will increase the use of copyrighted works in educational, non-profit archival, and preservation settings.

In 2018, the Acting Register determined that an exemption for good-faith security research is likely to "increase the use of works in educational settings."[132] Further, the Register noted in 2015 that the current prohibition plays a negative role in universities' willingness to engage in and fund security research and may limit student involvement in academic research projects."[133]

Removing the Other Laws and Use Limitations will increase the use of works in educational settings. The ambiguities in the current exemption introduce a risk of liability for students and teachers who do not have sufficient clarity concerning exactly what activities are allowed.[134] The majority of research and scholarship is conducted by academic researchers in educational settings, and these ambiguities hinder student involvement as students may be exposed to individual liability.[135] By removing the Other Laws and Use Limitations, bad actors will not be able to use Section 1201 to threaten faculty students, reducing the potential for uncertainty.

The ambiguity within the Other Laws limitation allows bad actors to leverage existing laws to deter unwanted criticism and scrutiny. Companies like Voatz exemplify vendors that use ambiguities in existing laws as a sword to deter unwanted criticism and scrutiny, not to protect their own copyright.[136] According to researchers who were threatened by Voatz after attempting to disclose vulnerabilities in good faith:

> To companies like Voatz, coordinated vulnerability disclosure is a mechanism that shields the company from public scrutiny by allowing it to control the process of security research. The fact that the MIT researchers discovered vulnerabilities that reflect poorly on Voatz's security only underscores the need for public scrutiny—what is simply a hassle to Voatz is a crucial warning flare to the public.[137]

Threats like these are real and persistent to many researchers. Section 1201's Other Laws restriction provides these bad actors with an avenue to assert

---

[132] 2018 Recommendation at 312.
[133] 2015 Recommendation at 310.
[134] See discussion infra, Item F.1 (Documentary Statement of Harri Hursti and J. Alex Halderman).
[135] *Id.*
[136] *See* Response to Voatz's Supreme Court Amicus Brief, *supra* note 26.
[137] *Id.*

illegitimate, but detrimental, claims. Security research is a critical part of our modern cybersecurity infrastructure, but vendors like Voatz can abuse laws like the DMCA to deter criticism, something that copyright law has long recognized as a legitimate fair use.[138]

If the DMCA is focused solely on copyright infringement rather than broader concerns, students and researchers can easily determine whether a threat of liability under the DMCA is legitimate. A broad exemption would increase educational access and improve the educational opportunities available for budding security researchers. Thus, this factor weighs in favor of granting the exemption.

iii. Granting the proposed exemption will allow greater research, commentary, criticism, reporting, and teaching of copyrighted works.

In both 2018 and 2015, the Office found that this factor weighed in favor of the good-faith security research exemption.[139] In fact, in 2015, the Register found that "research is at the core of the proposed exemption," and that enabling good-faith security research would promote further research in the future.[140]

All aspects of security research, from scholarship, teaching, and testing, to commenting, criticizing, and reporting, are disincentivized by the limitations and ambiguities in the current exemption. The resulting chilling effects inhibit or completely stop key security research, thereby undermining the security of critical information infrastructure and national security. In-progress research may be postponed or abandoned completely due to fears over liability; in such cases, legitimate research is deterred and vulnerabilities are allowed to manifest. There are many examples of such reluctance to engage in security testing.[141]

The deterrence of legitimate security research harms the public interest, as consumers will continue to use potentially harmful products if researchers are chased off of completing their research. This type of security research is integral to today's digital world and granting the proposed modification to the exemption will increase the critiques, comments, reporting, teaching, scholarship and research on critical information infrastructure. Thus, this factor weighs strongly in favor of granting the exemption.

---

[138] 2015 Recommendation at 300-303.

[139] 2018 Recommendation at 312. 2015 Recommendation at 310-11.

[140] 2015 Recommendation at 311.

[141] *See* Response to Voatz's Supreme Court Amicus Brief, *supra* note 26; *see also* EFF, *Letter at DEF CON for CFAA Reform* (Aug. 1, 2013) https://www.eff.org/document/letter-def-con-cfaa-reform (both describing the chilling effects of overbroad cybersecurity regulations have on security research).

iv. Granting the proposed exemption will not negatively affect the market for copyrighted works.

In both 2015 and 2018, the Office determined that this factor was neutral because granting the exemption was unlikely to adversely affect the market or the value of copyrighted computer programs.[142] Further, in 2015, the Register determined that the "effect of the exemption on the market for or value of copyrighted works would generally not be adverse."[143] Rather, the Register stated that it was "not truly a copyright concern" that the results of security research "could erode public confidence in the safety and security of products that are found to be flawed."[144] Because these market concerns are a product of the insecure computer programs themselves, they are outside of the purview of copyright law. The Register further noted that "knowledge of and ability to correct such flaws will in fact enhance the value of the software and products at issue."[145]

Removing the current Other Laws and Use limitations will not negatively affect the market for the original copyrighted work. In general, an exemption for security research actually has a positive net effect on the market for software and devices as more security research invites new, more secure products to enter the market. Even if the research furthered by this exemption might hamper the market for some software and devices by exposing weaknesses in their security, this effect will not be due to copyright infringement, as noted by the Register in 2015.[146] Any damage to the market for copyrighted works will result only from the exposure of inherent shortcomings in the works themselves. Thus, because copyright law does not govern this type of market activity, this factor cuts in favor of granting the exemption.

v. National cybersecurity concerns weigh in favor of granting the exemption.

In addition to the concerns about the First Amendment and the scope of the Office's authority discussed above,[147] the Office should consider the national cybersecurity policy priorities negatively affected by the existing exemption's narrow formulation.

Good-faith security research and testing are matters of national security policy. Without robust security testing, bad actors can exploit vulnerabilities in national computer programs to the detriment of the United States and its citizens. By

---

[142] 2018 Recommendation at 312, 2015 Recommendation at 311.

[143] 2015 Recommendation at 311.

[144] *Id.*

[145] *Id.*

[146] *Id.*

[147] See discussion *supra*, Item E.3.i.

granting the proposed exemption, the Copyright Office will be furthering an important and legitimate national security interest.

The potential harms of a national cybersecurity breach are not negligible or speculative. While national security concerns are present in many computer programs, the issue is readily apparent in voting systems. In 2017, the Central Intelligence Agency, the Federal Bureau of Investigation, and the National Security Agency released a report stating that Russian President Vladimir Putin "ordered an influence campaign in 2016 aimed at the US presidential election . . . [to] undermine public faith in the US democratic process" and that this influence campaign combined "covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media uses or 'trolls.'"[148] The report found that Russian actors intruded into state and local election boards as well as collected and disclosed significant information about American citizens.[149] The agencies further stated that the attack was intended to undermine the democratic order.[150]

The Central Intelligence Agency has again reported that similar efforts directed by Putin continued in the 2020 Presidential election.[151] There are existing security flaws in technology in voting systems that can be discovered by security researchers before foreign actors are able to exploit the vulnerabilities for their own benefit. Online voting systems, used in many states, leave votes vulnerable to undetectable manipulation by third parties.[152] Such vulnerabilities undermine the validity of election results, even when there is no manipulation, as officials cannot prove that the results are accurate.[153]

While nation-state actors intent on harming American elections will not be deterred by liability under Section 1201, good-faith researchers will. If good-faith researchers are not able to diligently test software from fear of undue liability, this leaves the country's vital infrastructure unnecessarily vulnerable to nefarious

---

[148] Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Report* at ii (Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf?utm_source=fbia.

[149] *Id.*

[150] *Id*.

[151] Julian E. Barnes & David E. Sanger, *Putin Most Likely Directing Election Interference to Aid Trump, C.I.A. Says*, N.Y. Times (Sept. 22, 2020), https://www.nytimes.com/2020/09/22/us/politics/cia-russian-election-interference.html.

[152] *E.g.,* Michael A. Spector & J. Alex Halderman, Security Analysis of the Democracy Live Online Voting System at 19 (June 7, 2020), https://internetpolicy.mit.edu/wp-content/uploads/2020/06/OmniBallot.pdf.

[153] *Id*. at 23.

actions. Granting the exemption will allow security researchers to find existing flaws to protect the United States from interference by foreign actors as well as establish trust in the electoral process

5. Section 1201's prohibition on circumventing access controls and the limitations in the existing exemption are the cause of the adverse effects.

The Use and Other Laws limitations in Section 1201 are the cause of the adverse effects detailed in the above section. These limitations are insufficiently clear and restrict uses that good-faith security researchers desire to undertake to increase the security in digital products. This lack of clarity chills security research resulting in societal harm. Moreover, non-circumventing methods often cannot achieve the same significant, worthwhile results as circumvention especially where circumvention itself is the process being researched. In most cases, there are no reasonable alternatives to circumvention as devices are protected by TPMs. As a result, without a broad exemption, good-faith security research will not be undertaken, and society will remain vulnerable to bad actors.

Section 1201 liability is being used as a sword to stop security research. Meanwhile, the shield of the current exemption does not protect researchers as it was intended. This harms not only the researchers but also the public. Accordingly, the Register should recommend, and the Librarian should grant the proposed modifications.

Item F. Documentary Evidence

1. Statement of Harri Hursti and J. Alex Halderman

We are security researchers who regularly work on—among many things—election integrity projects. Harri is a world-renowned security researcher who has conducted studies on election security in the United States and abroad. Harri previously exposed critical vulnerabilities in election systems such as the Diebold Voting System that allowed for the alteration of votes.[154] Alex is a professor of computer science and engineering at the University of Michigan. Alex's work includes software security, election cybersecurity, and cybercrime. Alex has published papers on a variety of cybersecurity issues from voting integrity to software exploits.[155]

The following is an example of the various legal regimes—including Section 1201—that have adverse effects on our research. For each law mentioned, there is significant uncertainty regarding what steps we must take to avoid prosecution or litigation for otherwise good-faith security testing. This uncertainty can lead us—

[154] Harri Hursti, Nordic Innovation Labs https://www.nordicinnovationlabs.com/about-us/harri-hursti/ (last visited Dec. 14, 2020)

[155] J. Alex Halderman, https://jhalderm.com/ (last visited Dec. 14, 2020)

and other security researchers—to abandon otherwise valuable projects out of caution or the inability to obtain informed legal counsel. While some of the specifics are unique this the example described below, all of the various legal regimes and problems mentioned below are frequently encountered by security researchers across the spectrum of potential projects.

Occasionally, vendors will ship voting machines with assurances that the machines cannot be accessed or controlled wirelessly. However, these machines may contain a wireless modem that has been switched off but could easily be activated by a malicious actor. In order to assess the potential vulnerabilities in machines like this that could allow for—among other things—the alteration of votes by malicious actors.

First, it is necessary to determine whether or not the device actually has a wireless modem. Obviously, it would be easiest to physically take apart the machine to determine this, but vendors often include contractual restraints that prevent purchasers from taking apart or fixing machines on their own. There may also be contractual provisions that prohibit buyers from re-selling devices to third parties.

This introduces two levels of uncertainty—first, whether or not the contract actually contains provisions that prohibit repair or resale, and second, whether conducting any tests on machines violates these contractual provisions. For example, if the contract includes a prohibition on resale it can make it much more difficult to legally obtain a machine to perform research on. As a researcher, it can often be impossible to determine whether or not a machine is subject to these kinds of contractual limitations, leading to uncertainty concerning legal liability.

It is possible to look for a wireless signal from the device using a software-defined radio (SDR), but this invites another potential set of issues. While attempting to locate a signal from the voting machine, all kinds of wireless signals may be received. In order to determine what devices are sending these signals it is necessary to actually view or interpret this data. This introduces uncertainty with regards to the Electronic Communications Privacy Act (ECPA). Even if the data is discarded as soon as it is determined to be from an unrelated device, there is still significant uncertainty regarding potential liability under ECPA.

Once the correct signal has been identified, trying to communicate with the machine and assess the potential vulnerabilities invites yet another legal issue. The notoriously vague CFAA prohibits accessing a “protected computer” either “without authorization” or in excess of “authorized access.” The definition of *all* of those terms is currently ambiguous, inviting even more uncertainty for security researchers who must frequently access devices without authorization in order to actually identify and understand potential vulnerabilities.

Finally, it may be necessary to circumvent a technological protective measure (TPM) in order to actually audit the software and expose a vulnerability. Circumventing a TPM is sometimes the only way to actually view the code

necessary to discover potential vulnerabilities. While this kind of circumvention may allow access to a copyrighted work, security researchers rarely, if ever, conduct this kind of circumvention for any purpose except to evaluate and understand potential vulnerabilities.

In sum, there are a number of complex legal questions that security researchers must answer before undertaking a project. It can be difficult to find counsel that can provide answers to the potential for liability under *any* of the above referenced laws, especially for academic researchers who have little to no funding for legal expenses. However, in the context of Section 1201, because of the Other Laws Limitations, it is necessary to find legal counsel with expertise in all of the above-mentioned regimes, as well as any potentially relevant state or local ordinances that may limit the ambit of permissible research. The Use Limitations also create uncertainty because it is ambiguous what kinds of post-circumvention conduct—such as publishing studies in an academic journal or discussing findings with the press—are considered within the scope of good-faith security research.

The uncertainty from these limitations can be particularly problematic for researchers studying systems used by firms deploying software solutions to traditionally analog technologies like election equipment. While most software companies are welcoming of security research, voting machine vendors and other similar firms can be particularly hostile to security research. For security researchers on the ground, a clearer and more concise exemption to Section 1201 would reduce uncertainty and provide ample breathing room for valuable research.