UNITED STATES COPYRIGHT OFFICE

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

Item A. Commenter Information

Commenter:

Prof. Ed Felten and Prof. J. Alex Halderman

Prof. Felten is a computer scientist whose research interests include computer security and privacy, and public policy issues relating to information technology—specifically, software security, Internet security, electronic voting, cybersecurity policy, technology for government transparency, network neutrality, and Internet policy.

Prof. Halderman is a computer scientist whose research focuses on computer security and privacy, with an emphasis on 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.

Representative:

Samuelson-Glushko Technology Law & Policy Clinic
Colorado Law

Blake E. Reid, Director
Elizabeth Field and Justin Manusov, Student Attorneys

Counsel to Prof. Felten and Prof. Halderman

blake.reid@colorado.edu
303-492-0548
Robert & Laura Hill Clinical Suite, 404 UCB Boulder, CO 80309-0404

Table of Contents

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

The above-referenced petitioners comment on Proposed Class 10: Computer Programs—Security Research.[1]

The Copyright Office initiated the seventh triennial rulemaking proceeding under the Digital Millennium Copyright Act (DMCA) on June 19, 2017 by issuing a Notice of Inquiry and Request for Petitions.[2] In response, the above-mentioned petitioners filed a Petition to Renew the Current Exemption for good-faith security research under 37 C.F.R. § 201.40(b)(7) on August 1, 2017.[3] In addition to the Petition to Renew, we filed a Petition for a New Exemption on September 13, 2017 to modify the current good-faith security research exemption under 37 C.F.R. § 201.40(b)(7).[4]

On October 26, 2017, the Copyright Office issued a Notice of Proposed Rulemaking (NPRM) for this proceeding.[5] In the NPRM, the Office announced that it "intends to recommend renewal of [the good-faith security research] exemption" in its current form.[6]

The current exemption, codified at 37 C.F.R. § 201.40(b)(7), exempts computer programs that operate devices and machines primarily designed for use by individual consumers (including voting machines), motorized land vehicles, or medical devices designed for implantation in patients and corresponding personal monitoring systems, for purposes of good-faith security research.[7] We appreciate the Office's renewal of the existing exemption.

[1] Exemptions to Permit Circumvention of Access Controls on Copyrighted Works, 82 Fed. Reg. 49,562 (proposed Oct. 26, 2017) (to be codified at 37 C.F.R. pt. 201) https://www.gpo.gov/fdsys/pkg/FR-2017-10-26/pdf/2017-23038.pdf (2017 NPRM).

[2] Exemptions to Permit Circumvention of Access Controls on Copyrighted Works, 82 Fed. Reg. 29,804 (proposed Jun. 30, 2017) (to be codified at 37 C.F.R. pt. 201). https://www.gpo.gov/fdsys/pkg/FR-2017-06-30/pdf/2017-13815.pdf (2017 NOI).

[3] Felten & Halderman Class 25 Renewal Petition Jun. 31, 2017. 2017. https://www.regulations.gov/document?D=COLC-2017-0007-0023 (2017 Renewal Petition).

[4] Felten & Halderman Class 25 Petition for New Exemption. Sept. 9, 2013 https://www.regulations.gov/document?D=COLC-2017-0007-0056 (2017 Modification Petition).

[5] 2017 NPRM, 82. Fed. Reg.

[6] *Id.* at 49,553.

[7] *Id.*

While renewing the existing exemption is a positive step toward enabling security research, it also introduces limitations on noninfringing good-faith security research and fails to address some of key ambiguities that chill good-faith security research. This petition seeks to modify and clarify the existing exemption by:

1. Removing the limitation that circumvention be undertaken on the specific categories of devices specified in 37 C.F.R. § 201.40(b)(7)(i)(A)-(C) (the "**Device Limitation**");
2. Removing the limitation that circumvention be "carried out in a controlled environment designed to avoid any harm to individuals or the public" (the "**Controlled Environment Limitation**");
3. Removing the limitation that circumvention be undertaken on a "lawfully acquired device or machine on which the computer program operates" and "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" (the "**Other Laws Limitation**");
4. Removing both references to the term "solely" from the provisions of the exemption in 37 C.F.R. § 201.40(b)(7)(i) and (ii), that limit circumvention to be 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" (the "**Access Limitation**");
5. Removing the limitation 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" (the "**Use Limitation**").[8]

The modifications would serve to further Congressional intent by promoting noninfringing good-faith security research in the spirit of Section 1201's existing security-related exemptions while addressing the problematic ambiguities and shortcomings of those exemptions and of the current good-faith security research temporary exemption.[9]

The Register noted in 2015 that "while Congress clearly foresaw the need to facilitate good-faith security research, it is less clear that the exemption has been as effective as it needs to be. Proponents of the security related exemptions have put forth a convincing case in this proceeding that [one of the existing statutory exemptions] does not provide enough certainty to ensure that certain types of legitimate research are able to move forward."[10]

[8] 2017 Modification Petition at 2–3.

[9] *See* 17 U.S.C. §§ 1201(f), (g), and (j); 37 C.F.R. § 201.40(b)(7).

[10] Register of Copyrights, Section 1201 Rulemaking: Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendation of the

Furthermore, in the Final Rule, the Librarian notes that "[t]he Register also concluded that the permanent exemptions in sections 1201(f), 1201(g), and 1201(j) are inadequate to accommodate the proposed research activities due to various limitations and conditions contained in those provisions."[11] Thus, similar limitations and conditions that are imposed in the current regulation should be removed in order to facilitate the Congressionally intended noninfringing security research.

Regarding the delayed effective date, the NPRM notes that the Office will remove language relating to a delayed effective date because the time delay for that exemption "was intended to be a one-time delay."[12] We agree that the expanded exemption should go into effect immediately upon the issuance of the final rule by the Librarian of Congress as required by Section 1201(a)(1)(D) without delay for all computer programs covered by the exemption and appreciate the Office's clarification to that effect.[13]

Item C: Overview

We live in a world that runs on software. It is difficult to imagine a world where people are not affected by software—from the things we touch, such as smartphones and tablets, to infrastructure that runs our everyday lives, like transportation and government. Software underlies the World Wide Web, vehicles, home appliances, our elections, and our life-saving medical devices.

The security of modern software and the devices that execute this software is thus of paramount importance for both the security of our nation and the security of our lives.[14] Yet software vulnerabilities expose us to a frighteningly high level of cybersecurity threats. In 2016, attacks against corporations and financial institutions increased; an average of 62 percent of financial threat detections were on consumer computers.[15] Ransomware infections increased by 36 percent between 2015 and 2016, and the United States is the

Register of Copyrights at 316 (Oct. 8, 2015), https://www.copyright.gov/1201/2015/registers-recommendation.pdf (2015 Recommendation).

[11] Exemptions to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65,944, 65,956 (proposed Oct. 28, 2015) (to be codified at 37 C.F.R. pt. 201), (2015 Final Rule).

[12] 2017 NPRM, 82 Fed. Reg. at 49,555 n.44.

[13] *See* 17 U.S.C. § 1201(a)(1)(D).

[14] Adam Gorlick, *Obama at Stanford: Industry, government must cooperate on cybersecurity*, Stanford News, Feb. 13, 2014 *available at* https://news.stanford.edu/2015/02/13/summit-main-obama-021315/.

[15] Symantec Corporation, *Financial Threat Review 2017*, 4 (2017), *available at* https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pdf.

country most affected by ransomware attacks.[16] From multi-million dollar bank heists to the disruption of the United States presidential election by state-sponsored groups, 2016 saw an unprecedented level of disruption through cyber-attacks and cyber espionage.[17]

To rectify these failings, it is critical that security researchers can work without fear of substantial legal liability to find and fix vulnerabilities in the software and devices on which we rely. In order to do this vital work, security researchers must occasionally bypass various measures designed to control access to software and devices.

While the anti-circumvention provisions of Section 1201 of the DMCA were intended to stop copyright infringers from defeating anti-piracy protections added to copyrighted works, the provisions have, in practice, chilled a wide array of legitimate security research activities. As a result, the DMCA has become a serious threat to several important public policy priorities including chilling free expression and scientific research, jeopardizing fair use, impeding competition and innovation, and interfering with computer intrusion laws.[18]

Our requested modifications to the exemption provisionally recommended for renewal in the NPRM build on that exemption, as well as the exemptions codified in the DMCA, seeking to unify them under one exemption to remove the ambiguity and other shortcomings that chill security research. We seek to ensure that circumventing technological protection measures (TPMs) on software and software-controlled systems is permitted for the full range of good-faith security research. Such an exemption would ease the burden of performing this class of research, ensuring that researchers are free to continue their work safeguarding and securing the range of software systems upon which we rely every day, including building automation systems, cryptographic banking, avionic network systems, traffic control infrastructure and cloud computing systems.

Moreover, granting these proposed modifications is largely consistent with the underlying analysis the Office relied upon in provisionally renewing the existing exemption and in granting similar exemptions for good-faith security research into sound recordings on compact discs during the 2006 proceeding and video games accessible on personal computers during the 2010 proceeding.[19] The expanded scope of security research that

[16] Symantec Corporation, *Ransomware 2017*, 4-6 (2017), *available at* https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf.

[17] Symantec Corporation, *Internet Security Threat Report*, 22 (2017), *available at* https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-JUN8.pdf?aid=elq_.

[18] Electronic Frontier Foundation, *Unintended Consequences – 16 years Under the DMCA*, Sept 16, 2014 *available at* https://www.eff.org/files/2014/09/16/unintendedconsequences2014.pdf.

[19] Exemption to Prohibited Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68,472 (Nov. 27, 2006) (codified at 37 C.F.R. pt. 201);

would be permitted under the proposed modifications do not change the relevant scope of TPMs, the reality that security research is non-infringing, or the resulting analysis favoring the grant of an exemption under Section 1201's statutory factors. Granting the modifications would merely highlight that the limitations in the existing exemption impose specific but significant adverse effects that should be remedied by removing the limitations in the final exemption.

The Device Limitation provides that circumvention may only be undertaken on specific categories of devices, namely, consumer devices, motorized land vehicles, and medical devices.[20] This limitation significantly harms noninfringing research because it is ambiguous as to what a consumer device is, and because the limitation prevents researchers from working on devices that are not included in this list.[21] These adverse effects in turn significantly chill research on these devices, leaving many important devices, such as building automation systems and commercial networking equipment, vulnerable to attack.[22]

The Controlled Environment Limitation provides that circumvention be "carried out in a controlled environment designed to avoid any harm to individuals or the public."[23] This limitation should be removed because it is ambiguous and because it prevents researchers from ensuring that systems are secure in real-life environments.[24] Often, researchers conduct investigations that include one or more unknown variables.[25] Because the Office has not explained what makes an environment "controlled," researchers are less likely to engage in such research because they may be exposed to liability.[26] Furthermore, some research needs to be conducted in real-life environments in order to ensure that the daily operation of such systems is not vulnerable.[27]

The Other Laws Limitation provides that circumvention be undertaken on a "lawfully acquired device or machine on which the computer program operates" and "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."[28] This limitation should be removed because it potentially exports the DMCA's harsh criminal and civil liability into other non-copyright legal regimes, exposing researchers to double liability. Furthermore, the Office

Exemption to Prohibited Circumvention of Copyright Protection Systems for Access Control Technologies, 75 Fed. Reg. 43,825 (July 27, 2010) (codified at 37 C.F.R. pt. 201.40).

[20] 37 C.F.R. § 201.40(b)(7)(i)(A)–(C).

[21] *See* discussion *infra,* Part E(3)(a) (Device Limitation).

[22] *See id.*

[23] 37 C.F.R. § 201.40(b)(7).

[24] *See* discussion *infra,* Part E(3)(a) (Controlled Environment Limitation).

[25] *See* discussion *infra,* Documentary Evidence (Felten and Halderman Personal Statement).

[26] *See* discussion *infra*, Part E(3)(a) (Controlled Environment Limitation) and Documentary Evidence (Felten and Halderman Personal Statement).

[27] *See* discussion *infra*, Part E(3)(a) (Controlled Environment Limitation).

[28] 37 C.F.R. § 201.40(b)(7).

overstepped its authority when it included this limitation because this limitation does not alleviate the harms of the prohibition against circumvention on noninfringing uses. In fact, it does the opposite: this limitation increases the adverse effects of the prohibition against circumvention on noninfringing security research.

The Access Limitation provides that research be done "solely" for the purpose of good-faith security research and "solely" for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability.[29] It is important to remove both references to the term "solely" in order to avoid restricting researchers' post-circumvention speech and also in order to allow researchers to investigate for purposes such as education and scholarship.[30]

The Use Limitation provides 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."[31] This limitation restricts researchers' First-Amendment protected speech by preventing researchers from using post-circumvention information for things like education, criticism, and scholarship.[32] Researchers sometimes discover systems with security flaws that are so fundamental to the software that the best way to protect consumers is for researchers to advise that they stop using these devices.[33] This limitation prevents researchers from protecting consumers from these underlying security vulnerabilities.[34]

Information security research benefits the public by making complex technologies more transparent and teaches the technology community how to design better, safer products in the future.[35] Removing these limitations would, in short, 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.

Item D: Technological Protection Measures and Methods of Circumvention

The 2015 record regarding TPMs related to computer security research was full and detailed.[36] In 2015, the Register concluded, "[b]ased on the overall record in [the 2015]

[29] *Id.*

[30] *See* discussion *infra*, Part E(3)(a) (Access Limitation).

[31] 37 C.F.R. § 201.40(b)(7).

[32] *See* discussion *infra*, Part E(3)(a) (Use Limitation).

[33] *See* discussion *infra*, Part E(3)(a) (Use Limitation) and Documentary Evidence (Felten and Halderman Personal Statement).

[34] *See* discussion *infra*, Part E(3)(a) (Use Limitation). and Documentary Evidence (Felten and Halderman Personal Statement).

[35] Slate Magazine, *The Chilling Effects of the DMCA*, Edward Felten, March 29, 2013 *available at* http://www.slate.com/articles/technology/future_tense/2013/03/dmca_chilling_effects_how_copyright_law_hurts_security_research.html.

[36] 2015 Recommendation at 305; 2015 Final Rule, 80 Fed. Reg. at 65,956.

proceeding" 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."[37] The Register also 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."[38]

This record is incorporated into the current proceeding through the Office's NPRM. In the NPRM, the Office determined that "the statutory language [of Section 1201] appears to be broad enough to permit determinations to be based upon evidence drawn from prior proceedings, but only upon a conclusion that this evidence remains reliable to support granting an exemption in the current proceeding."[39] The Office concluded that the evidence remains reliable by "intend[ing] to recommend readoption of all existing exemptions in their current form."[40] The Register determined that "due to a lack of legal, marketplace, or technological changes, the factors that led the Register to recommend adoption of the exemption in the prior rulemaking will continue into the forthcoming triennial period."[41] Therefore, the record from 2015 that established that TPMs have a significant impact on the ability to engage in good-faith security research is fully incorporated into this proceeding.

The relevant TPMs in this modification petition are the same as the TPMs described in the 2015 proceeding. Though the removal of some of the limitations, such as the Device and Controlled Environment Limitations, will lead to circumvention of new types of devices under new sets of circumstances, the categories of TPMs implicated are the same as the ones recognized previously by the Office.

Not every measure will necessarily qualify as a TPM under the meaning of Section 1201(a)(3)(B), depending on the specifics of its implementation. However, in 2015, the Comment of Matthew Green, among others, outlined 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."[42] These are still the types of TPMs that would be circumvented if the Office granted the requested removal of the modifications limitations.

[37] 2015 Recommendation at 305 (internal citations omitted).

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

[39] 2017 NPRM, 82 Fed. Reg. at 49,552 (citation omitted).

[40] *Id.* at 49,553.

[41] *Id.* at 49,552 (citation omitted).

[42] Matthew Green, Long-Form Comment Proposed Class 25 Security Research Docket No. 2014-07 at 5. https://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_Green_Class25.pdf (2014 Green Comment).

As the Green Comment explained:

> One class of measures is designed to control whether or not a user can install, execute, or otherwise use software or a device and the manner in which they may do so. In order to undertake good faith security research, it is essential to be able to install, execute and run a variety of legitimately obtained software or devices for a range of fair use purposes. Researchers must be allowed to circumvent protection measures aimed at controlling these capabilities, which include keys, shared secrets, usernames, passwords, external authentication or tethering systems, dongles, installation media, hardware fingerprinting, and license prompts or click-through dialogs.[43]
>
> . . . .
>
> A second class of measures is designed to control whether or not a user can read, inspect, or study software or a device. Being able to read, inspect, and study software is a critical component of finding and fixing security vulnerabilities. . . .[44]
>
> . . . .
>
> A third class of protection measures aims to control whether or not users can modify the underlying software or device to change the manner in which it operates. Whether it be in support of the previously discussed circumventions, or as the primary goal of their research, security researchers are often required to modify software or devices. The ability to modify obtained software is a key component of effective security research. . . .[45]
>
> . . . .
>
> A final class of protections simply aim to track software or a device, track the manner in which a user uses or modified software or a device, and/or report this data to external parties. While these techniques do not directly control or protect access to software or a device, they do serve to report the user's activities to an external party. There are a number of situations where security researchers would need to circumvent such mechanisms for the purpose of maintaining the confidentiality

[43] *Id.*

[44] *Id.* at 7.

[45] *Id.* at 9.

> of their research or as part of an investigation into the security of the tracking mechanism itself. . . .[46]

It is important that security researchers be able to find and fix security vulnerabilities in any software or device, even when they must circumvent both TPMs designed to protect the software or device itself (the primary class of works) as well as TPMs designed to protect additional works accessed via software or a device (the ancillary class of works). As the Green comment clarifies, the purpose of such ancillary circumventions is not to gain access to the additional protected works, but is instead an unavoidable consequence of, or requirement to, finding and fixing security vulnerabilities.[47] Rootkit-level protection on CDs or related sound recording media, or cryptographic protections on eBooks, software manuals, DVDs, or other media accessed via software-controlled devices are examples of such ancillary measures that security researchers may need to bypass.[48] The Copyright Office has granted such exemptions for bypassing TPMs on such works in the past for the purpose of good-faith security research.[49]

Item E. Asserted Adverse Effects on Noninfringing Uses

The Office encouraged commenters to focus on the following elements to demonstrate that proposed modifications to existing exemptions satisfy the requisite elements 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.[50]

The limitations that would be removed by the proposed modifications impose significant adverse effects on noninfringing security research. The proposed modifications do not change the underlying class of works in the existing exemption, which the Register concluded in 2015 includes at least some works protected by copyright.[51] The Register also concluded that good-faith security research is a noninfringing use, and the intended uses that

[46] *Id.* at 10.

[47] *Id.*

[48] *Id.*

[49] 2015 Recommendation at 319–20.

[50] 2017 NPRM, 82 Fed. Reg. at 49,511.

[51] *See* 2015 Recommendation at 299.

the modifications would enable do not differ in any way material to the question of infringement.[52]

Researchers are adversely affected in their ability to conduct such noninfringing use. The Device and the Controlled Environment Limitations adversely affect noninfringing research because they are ambiguous and because they prevent noninfringing research on certain devices or in certain environments.[53] The Other Laws Limitation adversely affects noninfringing research by introducing multiple surfaces of liability from non-copyright legal regimes.[54] The Access and Use Limitations adversely affect noninfringing research by preventing researchers from using the derived information for scholarship, for teaching, and for effectively protecting consumers from flawed devices.

In 2015, 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 exemption are slightly different, the adverse effects are similarly directly caused by the prohibition on circumvention.[55]

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

The Register concluded in her 2015 Recommendation that "good-faith testing for and the identification, disclosure and correction of malfunctions, security flaws and vulnerabilities in copyrighted computer programs have been hindered by TPMs that protect those programs."[56] 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]."[57] 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 2015, the Register determined that good-faith security research was likely to be a non-infringing use. Most computer security research does not implicate copyright because the underlying material is either not copyright protected or is a weak copyright because the underlying work is functional. If the underlying work is found to be copyright-protected, the security research may be a noninfringing use under Section 117, as the Register determined with respect to security research on vehicle software in 2015. Lastly, if the underlying work is

[52] *Id.* at 300.

[53] *See* discussion *infra*, Part E(3)(a) (Device Limitation and Controlled Environment Limitation) and Documentary Evidence (Felten and Halderman Personal Statement).

[54] *See* discussion *infra*, Part E(3)(a) (Other Laws Limitation) and Documentary Evidence (Felten and Halderman Personal Statement).

[55] 2015 Recommendation at 299.

[56] *Id.*

[57] 2015 Final Rule, 80 Fed Reg. at 65,956.

found to be copyright-protected, the security research will be fair use, just as the Register determined that security research was fair use in 2015.

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

A significant proportion of computer security research does not constitute an infringing act because it simply involves accessing functional, non-copyrighted elements of the works. Functional elements of copyright works are separate from the copyrighted elements of that work.[58] Although software and devices contain both creative and functional elements, legitimate computer security researchers focus on the functional elements. The functional elements, such as a computer program's object code, which contains ideas and executes tasks, are excluded from copyright protection.[59] Computer programs are protected to a lower degree than traditional literary works because they "contain unprotected aspects that cannot be examined without copying."[60]

Moreover, in most security research, nothing is reproduced, distributed, or adapted. Most relevant security research focuses not on the reproduction, distribution, or adaptation of copyrighted works, but on the investigation of those works. In the course of good-faith security research, there may be some incidental reproduction, distribution, or adaptation, but that reproduction will almost certainly be ancillary to the research.

In her 2015 Recommendation, the Register agreed that the computer programs at issue in the existing exemption are "likely to fall on the functional rather than creative end of the spectrum."[61] The Register explained, "When a computer program is being used to operate a device, the work is likely to be largely functional in nature, as in the case of a cellphone's operating system, software contained in a vehicle's ECU, or software used to control a medical device."[62]

None of the proposed modifications lead to a different conclusion. The underlying works that researchers will access are not likely to be protected by copyright because they are largely functional in nature.

b. Even if computer security research does implicate copyright, it may be a noninfringing use under Section 117.

Section 117 provides that "it is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that

[58] *Sega Enterprises Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992), as amended (Jan. 6, 1993).

[59] *Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596, 602 (9th Cir. 2000) (citing 17 U.S.C. § 102(b)).

[60] *Id.*

[61] 2015 Recommendation at 301.

[62] *Id.*

computer program provided (i) that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner, or (ii) that such new copy or adaptation is for archival purposes only and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful."[63]

The Office has already determined that "many of the security research uses proposed for owners of vehicles may quality as protected uses under section 117."[64] The Register also noted that "regardless of whether research technically qualifies as noninfringing under section 117, that provision highlights Congress's general view of the importance of users' ability to copy and adapt the computer programs they own to enhance their usefulness, and reinforces the conclusion that such uses here are likely to be fair."[65] To the extent that security research performed on software outside the context of vehicles meets the ownership requirement and meets the essential step requirement, it is a noninfringing use under Section 117.

Furthermore, as the Register noted, the policy underlying Section 117 highlights Congress's general view of the importance of users' ability to copy and adapt computer programs they own to enhance their usefulness. The Device and Controlled Environment Limitations contradict that general view because they prevent researchers from circumventing certain devices and from circumventing in certain environments, respectively. Thus, the Office should grant the petition's modifications which create a broad security research exemption so that such noninfringing research may be done without fear of liability under the DMCA.

c. Even if computer security research does implicate copyright and is not eligible for Section 117, 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. Fair use includes four factors: (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.[66]

In 2015, the Register determined that good-faith security research was likely to be fair use, noting that "accessing and reproducing computer programs for purposes of facilitating

[63] 17 U.S.C. § 117.

[64] 2015 Recommendation at 305.

[65] *Id.*

[66] 17 U.S.C. § 107.

good-faith security research and identification of defects are likely to be fair uses."[67] The uses proposed by this modification petition are the same as those uses proposed in 2015.

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.[68] While it is difficult to 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.[69] Importantly, the proposed exemption does not seek to insulate activities that go beyond security research.

Purpose and character. The purpose and character of the intended uses weigh in favor of fair use. The purpose and character of a use is determined by whether the use is transformative rather than merely derivative, whether the use is for educational purposes, and if the use is for commercial use.[70] Whether a work is transformative depends on "whether the new work merely supersede[s] the objects of the original creation, or instead adds something new, with a further purpose or different character, altering the first with new expression, meaning, or message;" it asks, in other words, whether and to what extent the new work is transformative.[71]

In 2015, the Register determined that many of the proposed uses are "likely to be transformative, including copying the work to perform testing and research."[72] The Register determined that "[i]n many cases the purpose of the use is to engage in academic inquiry."[73] The Register found that the desired research activities "may result in criticism or comment about the work and the devices in which it is incorporated, including potential flaws and vulnerabilities." The Register concluded that "in many cases, research activities may also extend to evaluating and describing how to fix flaws that have been discovered." Thus, the Register noted, good-faith security research "encompasses several of the favored activities listed in the preamble of section 107."[74] Furthermore, in 2010, the Register noted that "socially productive, transformative uses performed solely for good faith testing,

[67] 2015 Recommendation at 300.

[68] The Office should note that the Other Laws Limitation in the context of the fourth factor is not required in order to find that the underlying market is not effected by security research. *See* discussion *infra*, Part E(2)(c) (Effect on the relevant market).

[69] *See* 17 U.S.C. § 1201(c).

[70] *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 570 (1994).

[71] *Id.*

[72] 2015 Recommendation at 300.

[73] *Id.*

[74] *Id.*

investigation . . . of security flaws or vulnerabilities weigh heavily in favor of fair use under the first factor."[75]

Here the same analysis should be followed because the intended uses encompassed by the proposed modifications are of the same purpose and character as the intended uses in the existing exemption. The purposes of good-faith computer security research are all listed as paradigmatic fair uses in Section 107's preamble: criticism, comment, news reporting, teaching, scholarship, or research, and these paradigmatic fair uses are being restricted by the current exemption.

When good-faith computer security researchers investigate and discover security flaws and vulnerabilities in software or devices, they engage in scholarship or research. This noninfringing research is currently restricted by the Device Limitation, which limits noninfringing research to certain sets of devices.[76] This noninfringing research is also restricted by the Controlled Environment Limitation, which prevents researchers from studying vital infrastructure that can only be tested in the field or other arguably uncontrolled environments.[77]

When researchers document and responsibly disclose security flaws and vulnerabilities they engage in criticism, commentary, or news reporting. This noninfringing criticism, commentary, or news reporting is currently restricted by the Device Limitation because research is limited to certain sets of devices.[78] It is also directly restricted by the Use Limitation, because the Use Limitation potentially restricts researchers from using the information derived from noninfringing research in post-circumvention criticism, commentary, or news reports.[79] The Controlled Environment Limitation also restricts noninfringing criticism, commentary, and news reporting by chilling research in areas that need to be examined in uncontrolled environments.[80] Finally, noninfringing criticism, commentary, and news reporting is restricted by the Access Limitation, which chills activities that use the post-circumvention results of that noninfringing research.[81]

When professors permit students to perform hands on investigations of software or a device's security flaws and vulnerabilities the professors are engaging in teaching and education.[82] This noninfringing teaching and education is restricted by the Access and Use

[75] 2015 Recommendation at 300 (citing Recommendation of the Register of Copyrights, RM 2008-8 (2010), https://www.copyright.gov/1201/2010/initialed-registers-recommendation-june-11-2010.pdf).

[76] *See* discussion *infra*, Part E(3)(a) (Device Limitation).

[77] *See* discussion *infra*, Part E(3)(a) (Controlled Environment Limitation).

[78] *See* discussion *infra*, Part E(3)(a) (Device Limitation).

[79] *See* discussion *infra*, Part E(3)(a) (Use Limitation).

[80] *See* discussion *infra*, Part E(3)(a) (Controlled Environment Limitation).

[81] *See* discussion *infra*, Part E(3)(a) (Access Limitation).

[82] *See* discussion *infra*, Part E(3)(a) (Access Limitation).

Limitations.[83] Thus, the first factor weighs heavily in favor of fair use, and each limitation should be removed because they restrict noninfringing use.

Nature of the works. In 2015, the Register determined that this factor weighs in favor of fair use. The degree of creativity involved in the original work, as well as whether or not the original work has been published, both play a role in the second factor of a fair use determination.[84] The more factual and less creative a work, the more likely it is to be subject to fair use.[85] Publishing also increases the likelihood that a work is subject to fair use.[86] The Register reasoned that a computer program is likely to be "largely functional in nature" when it is being used to operate a device.[87] Thus, the Register determined that "the computer programs at issue are likely to fall on the functional rather than creative end of the spectrum."[88]

The nature of the works impacted by this modification petition is the same as the nature of the works proposed in 2015; the underlying copyrighted work is a computer program. Removing the Device Limitation expands the types of devices researchers may investigate; however, it will not alter the analysis of this factor because the underlying work remains a computer program.[89] Similarly, removing the Controlled Environment Limitation expands the types of investigation researchers may conduct; however, it does not alter the analysis under this factor because the underlying work remains a computer program.[90] Thus, this factor weighs in favor of fair use.

Amount and substantiality. The third factor asks whether the secondary use employs more of the copyrighted work than is necessary, and whether the copying was excessive in relation to any valid purposes asserted under the first factor.[91] For some purposes, it may be necessary to copy the entire copyrighted work, in which case the third factor does not weigh against a finding of fair use.[92] So long as the copying is required for a valid use and results in some form of "transformation," courts lean in favor of fair use.[93]

[83] *See* discussion *infra*, Part E(3)(a) (Access Limitation and Use Limitation).

[84] *Sega Enterprises Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1524 (9th Cir. 1992), as amended (Jan. 6, 1993).

[85] *Id.*

[86] *Id.*

[87] 2015 Recommendation at 301.

[88] 2015 Recommendation at 301.

[89] *See* discussion *infra*, Part E(3)(a) (Device Limitation).

[90] *See* discussion *infra*, Part E(3)(a) (Controlled Environment Limitation).

[91] *Campbell*, 510 U.S. at 586–87.

[92] *Authors Guild, Inc. v. HathiTrust*, 755 F.3d 87, 98 (2d Cir. 2014).

[93] *See Cariou v. Prince*, 714 F.3d 694, 710 (2d Cir.) cert. denied, 134 S. Ct. 618(2013); *Authors Guild Inc.,* 755 F.3d at 710; *Authors Guild, Inc. v. Google Inc.*, 954 F. Supp. 2d 282, 292 (S.D.N.Y. 2013).

In 2015, the Register found that this factor is consistent with a finding of fair use. The Register reasoned that "where functional elements of a computer program cannot be investigated or assessed without some intermediate reproduction of the works, courts have held that the third factor is not of significant weight."[94] The Register found that such copying was consistent with fair use in the 2006 and 2010 proceedings regarding researching compact discs and video games, respectively.[95] Thus, the Register determined that even if the third factor "disfavors a fair use finding, the weight to be given to it under the circumstances is slight."[96]

The Office has provisionally recommended renewal of the good-faith security research exemption in the NPRM, affirming again that such security research is noninfringing.[97]

The analysis under this factor is the same as in 2015 because the modifications do not change the amount or substantiality of use. Good faith researchers' investigations of security flaws and vulnerabilities often utilize few or none of a piece of software's copyrighted elements. When security research does require the copying of protected elements, that copying is merely incidental to the goal of the research, and is necessary to adequately investigate security concerns. When security research is published, it does not contain substantial portions of the original copyrighted work, and has completely transformed the copyrighted work for a significantly different use than the original. Because the works used are necessary to complete the research, and any published aspects are transformed by this research, the third factor weighs in favor of fair use.

Effect on the relevant market. The Supreme Court has described the fourth factor as "undoubtedly the single most important element of fair use."[98] The fourth factor looks at "the effect of the use upon the potential market for or value of the copyrighted work," and whether the secondary use "usurps the market of the original work." [99] In 2015, the Register found that this fourth factor weighs in favor of fair use.

The market for the original work here is the market for the software that is the focus of the research, since there is no protectable market for criticism or commentary.[100] The Register reasoned that "speculative concerns regarding reputational harms" are not the "concern" of copyright.[101] Rather, the Register found that the intended research will not

[94] 2015 Recommendation at 301.

[95] *Id.*

[96] *Id.*

[97] 2017 NPRM, 82 Fed. Reg. at 49,555.

[98] *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 567, 105 S. Ct. 2218, 2234 (1985).

[99] 17 U.S.C. § 107(4); *NXIVM Corp. v. Ross Institute,* 364 F.3d 471, 482 (2d. Cir. 2004).

[100] *Campbell*, 510 U.S. at 592.

[101] 2015 Recommendation at 302.

usurp the market for any original works because the researchers will be lawfully obtaining copies of those works for analysis.[102]

Good faith security research will not usurp the market for any original works subject to said research. Security research is not a replacement for any software, but only serves to criticize or comment on the security features of that software, which is a transformative act. Although a computer program or software company might suffer economic or reputational harm because its product's security flaws or vulnerabilities were disclosed, that harm is irrelevant since it does not usurp the original market.[103] Much of that harm will likely be avoided through coordinated disclosure with the company and the net result will be positive since this will lead to a market for works with more robust security. Thus, the fourth factor weighs in favor of a fair use determination.

The Register relies in part on the assumption that the tested copies will be lawfully obtained, as specified in the Other Laws Limitation, in order to find that this fourth factor weighs in favor of fair use.[104] However, this reliance does not need to be codified by including the "lawfully acquired" wording that exists in the current exemption. There is no record indicating that researchers ever intend to work on unlawfully obtained devices. However, there is a significant risk that researchers will obtain devices through legal means and later be threatened by liability due to an unknown third-party no-resale contract.[105] The Office should therefore not rely on including the "lawfully obtained" language to determine that this factor favors fair use.

3. Researchers are adversely affected in their ability to make noninfringing uses and are likely to be adversely affected in their ability to make such noninfringing uses during the next three years.

The current exemption's limitations have significant adverse effects on noninfringing security research. Each of the statutory factors that Congress lists in Section 1201 weighs in favor of removing the limitations.

a. The current exemption's limitations have significant adverse effects on noninfringing security research.

In 2015, the Register "conclude[d] 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."[106] The Register noted that a "significant number of product manufacturers employ TPMs on computer programs," and that "in many instances these TPMs have an

[102] 2015 Recommendation 301–302.

[103] *Id.* at 302.

[104] *Id* at 301–02.

[105] *See* discussion *infra*, Part E(3)(a) (Other Laws Limitation).

[106] 2015 Recommendation at 305.

adverse impact on the ability to engage in security research."[107] The Register concedes that "significant independent research is taking place through the cooperation of copyright owners," but emphasizes that "despite the existence of authorized research," adverse effects persist.[108]

The Register also concluded that Section 1201's built-in exemptions are insufficient to protect the interests of security researchers. She explained:

> The Register therefore concludes that, based on the current record, the permanent exemptions embodied in sections 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.[109]

Researchers experience adverse effects from the limitations within the current exemption for many various reasons and in different ways. The following sections describe the adverse effects that are specific to the Device Limitation, the Other Laws Limitation, the Controlled Environment Limitation, the Access Limitation, and the Use Limitation.

The Device Limitation. The Device Limitation provides that security researchers may only perform research on three specific classes of devices:

a. A device or machine primarily designed for use by individual consumers (including voting machines);

b. A motorized land vehicle; or

c. A medical device designed for whole or partial implantation in patients or a corresponding personal monitoring system, that is not and will not be used by patients or for patient care.[110]

The Device Limitation limits security researchers because its scope is ambiguous. The most significant ambiguity in the limitation is the reference to a "device or machine primarily designed for use by individual consumers."[111] In the 2015 rulemaking, the Office largely remained silent as to the contours of this limitation.

First, there is no explanation of what "primarily designed for" means. A narrow interpretation might focus an inquiry into the device developer's state of mind in creating the device. On the other hand, a broader interpretation might focus objectively on whether the devices is indeed used by consumers regardless of the developer's intent.

[107] *Id.*

[108] *Id.* at 305–306.

[109] *Id.* at 309.

[110] 37 C.F.R. 201.40(b)(7)(i)(A)–(C).

[111] 37 C.F.R. 201.40(b)(7)(i)(A).

Likewise, the Office offers no explanation of what "use by individual consumers" means. It is unclear whether this will be interpreted narrowly to refer to any device that a consumer individually and directly purchases, owns, and uses, such as a personal computer, or if it will be interpreted broadly to incorporate any device that a consumer indirectly uses or is a part of a larger system that a consumer interacts with.[112]

Taken together, these ambiguities render unclear the precise scope of this limitation. Does it apply to devices, such as commercial networking equipment, that might be intended by their vendors for enterprise customers but *could* be used by individual consumers? Does it include devices indirectly used by consumers, such as cryptographic banking tokens that underpin the operation of automatic teller machines? The rule provides little guidance as to how to answer these questions.

The resulting uncertainty chills security research because researchers are less likely to take on projects that may fall outside the narrowly construed scope of a consumer device to avoid potential liability.[113] Furthermore, this limitation directly chills researcher's ability to teach effectively, because there are ethical challenges in exposing student researchers to the same risk.[114]

There are several important examples of research projects that researchers avoid because the consumer device category is ambiguous. These examples fit a broad interpretation of consumer devices, in that they are systems that are indirectly used by consumers:

- **Building automation systems**. A building automation system is the automatic centralized control of a building's heating, ventilation and air conditions, lighting and other systems. In commercial buildings, many people affected by a building automation system do not purchase or own the system; even in residential buildings, such as apartments or even homes, automation systems may be purchased and installed by landlords, professional contractors, and other users who might not qualify as "consumers" under a narrow construction of the term. However, consumers undoubtedly rely upon and benefit from the use of such systems every time they inhabit a building that has one.[115]
- **Commercial networking equipment**. Commercial networking equipment is used by Internet service providers and related entities, although consumers rely upon it to pass their traffic to and from its destination.[116]

[112] *See* discussion *infra*, Documentary Evidence (Felten and Halderman Personal Statement).

[113] *See* discussion *infra*, Documentary Evidence (Felten and Halderman Personal Statement).

[114] *See* discussion *infra*, Part E(3)(b) and Documentary Evidence (Felten and Halderman Personal Statement).

[115] *See* discussion *infra*, Documentary Evidence (Felten and Halderman Personal Statement).

[116] *See* discussion *infra*, Documentary Evidence (Felten and Halderman Personal Statement).

- **Traffic control systems**. These systems are not available for individual consumer purchase. However, consumers rely heavily on traffic systems functioning properly.[117]
- **Avionics systems**. Avionics systems include ground to air communications and on-board networks. Avionics systems are directly and indirectly used by consumers. Flight passengers directly use avionic systems when they use in-flight WiFi. Passengers indirectly benefit from avionics systems because avionics systems enable safe transportation.
- **Drones**. Unmanned aerial vehicles all rely on software control systems and run the gamut from inexpensive devices that can be purchased by consumers in department stores to sophisticated scientific and military craft.
- **Cryptographic hardware modules.** These modules underpin the operation of certain banking systems.
- **Cyber-physical systems**. These systems are smart systems that include engineered interactions between networks of physical and computational components.[118]
- **Internet of Things**. The Internet of Things comprises a wide range of devices both sold to computers and integrated in commercial, industrial, and governmental applications.[119]
- **Industrial control systems**. This category includes Supervisory Control and Data Acquisition systems, Distributed Control Systems, and other control system configurations such as Programmable Logic Controllers. [120]
- **Devices that interact with the public Internet, but are unknown to researchers**. When researchers conduct Internet-wide scanning, they may interact with devices that may not be consumer devices. The ZMap Project is a "collection of open source tools that enables researchers to perform large-scale studies of the hosts and services that compose the public Internet."[121]

[117] *See* discussion *infra*, Documentary Evidence (Felten and Halderman Personal Statement).

[118] Cyber Physical Systems Public Working Group (CPSPWG), National Institute of Standards and Technology (NIST) *Framework for Cyber-Physical Systems Release 1.0,* May 26, 2016 *at* xiii, https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf (CPSWG 2016).

[119] *Id.*

[120] National Institute for Standards and Technology, *Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 80-82 Revision 2,* Stouffer, Keith. et. al., May 2015, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[121] *See generally* The ZMap Project 2017, https://zmap.io/.

To the extent the Office did not intend to include these types of devices within the Device Limitation, it must remove the limitation to ensure that researchers can pursue critical research projects to discover and mitigate vulnerabilities.

To the extent that the Office intended to remove these or other categories of devices—such as the nuclear power plants, smart grids, industrial enterprises, air traffic control functions, train systems, or traffic lights referenced in the 2015 recommendation—it should still remove the limitation. Computer security researchers, including Prof. Felten and Prof. Halderman, are concerned about and interested in exploring vulnerabilities in these types of devices, but choose not to do so in part because the scope of the Device Limitation is unclear.[122] This bona fide interest in pursuing research on a broad category of devices that would otherwise be subjected to Section 1201 is sufficient for the Office to eliminate the Device Limitation.

The Controlled Environment Limitation. The Controlled Environment Limitation requires that security research be conducted in a controlled setting designed to avoid harm to individuals or the public. But as implemented, the Controlled Environment Limitation can, paradoxically, harm individuals and the public because it is likely to chill safe and important research.

The Office provided little guidance about the contours of this limitation, nor is it well-positioned to do so. Establishing the contours of scientific methodology, including defining the contours of necessary controls on research lies nowhere near the ambit of copyright law or policy. Scholarly peer review, on the other hand, helps validate research and establishes methods by which the scientific method can be evaluated. Peer review constitutes a form of self-regulation by qualified members of a profession within the relevant field. The Office is not the appropriate body to improve the quality, uphold the standards, or provide certification in information security research.

The goal of good-faith information security research is to increase scientific understanding of the world we live in and the technology we interact with. One way scientists make sure their research avoids public harm is by improving internal validity—the extent to which the effects observed in the study are due to the intended manipulation of the desired variable—the independent variable—and not some other factor. Likewise, effective research depends on external validity—the extent to which the results of a study can be generalized to other settings (ecological validity) and other people (population validity) and over time.

The Controlled Environment Limitation adversely affects researcher's ability to generalize from data and theories applied in the laboratory to the real world outside the lab. The Controlled Environment Limitation, therefore, inhibits researchers from conducting experiments in which the environment must necessarily be uncontrolled. For example, information security researchers, with the consent of the device or system administrator, employ live testing to profile the real-world security of certain systems. Freeing researchers

[122] *See* discussion *infra*, Documentary Evidence (Felten and Halderman Personal Statement).

from the burden of controlling every variable in scientific experimentation allows researchers to observe unanticipated variables and confounding factors and to prove that what takes place in the lab can be generalized to what takes place "out there" in other settings. Improving external validity is designed to avoid harm to individuals and the public by improving the generalizability of scientific researcher. Research in uncontrolled environments allows researchers to measure variables from undetected sources, clarify causation from correlation, and improve reliability and verification.

Information security research on avionic control systems, for example, would be forestalled if researchers could not study how an airplane's on-board security systems interact with other planes and airports' control towers in real-time. An aircraft's Internet connectivity can be a direct link between the aircraft and the outside world, exposing avionic systems to unauthorized remote access while the aircraft is in flight. It is possible to conduct such research safely outside of the confines of a laboratory.

For example, a Department of Homeland Security (DHS) employee remotely hacked a Boeing 757 through radio frequency communications on September 21, 2016. The DHS official and team members were not present in the aircraft, nor did the hack occur in a laboratory.[123] This important research could only occur because the employee apparently was eligible for the government employee exemption in Section 1201(e), which has no controlled environment limitation.[124]

In another example, Internet-wide scanning, security researchers are studying the Internet itself.[125] This may involve making small numbers of harmless connection attempts to every publicly accessible computer each day. This allows researchers to measure the global Internet and analyze trends in technological deployment and security. These may consist of standard connection attempts followed by RFC-compliant protocol handshakes with responsive hosts. The data collected through these connections would consist solely of information that is publicly available on the Internet.[126] By analyzing the data from these scans, researchers can detect vulnerabilities in remote systems, or even entirely new classes of vulnerable systems, without physically interacting with any of the devices.[127] None of this research takes place within the confines of a lab.

[123] CSOOnline, *Homeland Security team remotely hacked a Boeing 757*, Ms. Smith, *available at* https://www.csoonline.com/article/3236721/security/homeland-security-team-remotely-hacked-a-boeing-757.html.

[124] *See* 17 U.S.C. § 1201(e).

[125] *See* Zakir Durumeric, Michael Bailey, & J. Alex Halderman, *An Internet-Wide View of Internet-Wide Scanning* (2014) Proceedings of the 23rd USENIX Security Symposium, http://web.engr.illinois.edu/~mdbailey/publications/usesec14_scanning.pdf.

[126] *See* discussion *infra*, Documentary Evidence (Felten and Halderman Personal Statement).

[127] *See e.g.* Zakir Durumeric, Frank Li, et al., *The Matter of Heartbleed* (2014) Proceeding of the 14th ACM Internet Measurement Conference; Nadia Heninger, Zakir Durumeric, Eric Wustrow & J. Alex Halderman, *Mining Your Ps and Qs: Detection of Widespread Weak Keys in*

Likewise building automation systems that deal with environmental controls—heating ventilation, air conditioning, lighting and shading—are increasingly becoming integrated and so they demand an integrated security protocol, rather than an isolation subsystem security protocol. In order to understand the inherent synergies between these diverse systems and protect against malicious interferences, information security researchers need to understand the security architecture of these systems in a real-time and real-world setting to detect and prevent any harm to individuals or the public.[128] Other examples include data breach analysis in Virtual Private Networks (VPNs) and other commercial networking equipment to research malicious payloads delivered to government-owned computers.[129]

Researchers need to both understand the capabilities and limitations of controlled and uncontrolled environments in information security research to protect individuals and the public. Removing this limitation positions information security researchers who are qualified and impartial to self-regulate their scientific practice and scholarship.

The Other Laws Limitation. The Other Laws Limitation provides that security research must be undertaken on a "lawfully acquired device or machine on which the computer program operates" and "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."[130] The Office should remove this limitation to avoid potentially exporting the significant civil and criminal liability in Sections 1203 and 1204 of the DMCA to other non-copyright legal regimes.

While the adoption of the existing exemption has mitigated a significant amount of the chilling effect of Section 1201 on good-faith security research, the Other Laws Limitation still chills research by calling into question the lawfulness of the acquisition of software and the lawfulness of the security research.

First, the "lawfully acquired" language brings into the ambit of Section 1201 enforcement disputes about the propriety of acquiring certain types of equipment that may bear no relationship to copyright infringement. For example, the vendor of a piece of commercial networking equipment might purport to bar the original purchaser from reselling the equipment in a sales contract. If the original purchaser later sells the equipment on EBay and it's purchased by a security researcher, the vendor might argue that the machine was unlawfully acquired, even though the security researcher had no knowledge or reason to know of the agreement between the vendor and the original purchaser. As a result, there might be a legal dispute that ensues over the resale of the equipment. Those types of disputes have nothing to do with copyright infringement or circumvention of TPM on the

Network Devices (2012) Proceeding of the 21st USENIX Security Symposium, https://factorable.net/weakkeys12.extended.pdf.

[128] *See* discussion *infra*, Documentary Evidence (Felten and Halderman Personal Statement).

[129] *See* discussion *infra*, Documentary Evidence (Felten and Halderman Personal Statement).

[130] 37 C.F.R. 201.40(b)(7)(i).

equipment's software and can and should be addressed in other contexts without raising questions of liability under federal anti-circumvention law.

Second, the Other Laws Limitation remains inappropriate because security research may raise complex questions under the Computer Fraud and Abuse Act (CFAA), state contract law, and federal regulatory regimes such as those governing medical and telecommunications equipment. Those regimes may have significantly different penalty structures, enforcement mechanisms, and judicial interpretations, and those complexities should be sorted out in other contexts without importing the DMCA's significant penalties.[131] It is beyond the Office's authority in the narrow ambit of this rulemaking to manage the interpretation of these other laws. Moreover, removing the Other Laws Limitation does not preclude liability under other applicable laws where researchers contravene the bounds of public policy. The Office is not the appropriate body, nor the Section 1201 rulemaking the appropriate forum, to address complex and controversial issues related to the policy governing security researchers.

The Access Limitation. Removing the two-pronged "Access Limitation" avoids limiting security researchers' broader aims, including teaching, scholarship, and research. First, removing both references to the term "solely" from the provisions of the exemption would avoid unconstitutionally limiting post-circumvention First-Amendment-protected speech. Second, removing "solely" would avoid including other non-infringing incidental activities derived from good-faith security research.

The existing exemption allows researchers to access computer programs "solely for the purpose of good-faith security research," which means in relevant part "solely for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability." In 2015, the Register did not give any specific justification regarding 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."[132] Indeed, the usage of "solely" in the Access Limitation tracks exactly with the use of "solely" in section 1201(j).[133]

This suggests that the Register included the word "solely" for the limited reason of tracking Congress's wording in the permanent exemption. This reasoning is insufficient to justify the significant adverse effects that the Access Limitation imposes on noninfringing security research.[134]

Congress did not ask the Office to merely mimic their own permanent exemptions, nor does the 2015 Recommendation justify doing so. Indeed, it would not have been necessary

[131] The DMCA's penalties include imprisonment under the provisions of Section 1204.

[132] 2015 Recommendation at 319.

[133] *See* 17 U.S.C. § 1201(j).

[134] *See* discussion *supra,* Part E(3)(a) (Access Limitation).

for Congress to delegate the authority to create new exemptions if the permanent exemptions were sufficient to protect against future harm. Rather, Congress entrusted the Office to create exemptions that protect noninfringing use from unanticipated future harms.[135]

Removing the term "solely" from the exemption limitations to a circumvention performed "for the purpose of good-faith security research" allows researchers to circumvent TPMs in furtherance of scientific dialogue, academic peer review, and classroom teaching. The word "solely" does not clarify whether activities that use the results of the noninfringing testing and investigation—for example, publishing papers—are covered. This ambiguity chills research and the resulting comments or reporting because researchers are hesitant to open themselves up to the threat of liability.

The Use Limitation. The Use Limitation 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."[136] The Use Limitation adversely affects security researchers because it is ambiguous, limits several noninfringing uses, and conditions eligibility for the exemption on the behavior of third-parties whom they cannot control.

The Use Limitation is ambiguous particularly in the context of the word "primarily." For example, a narrow reading might interpret "primarily" to mean "only"—such that if a researcher is found to have used the information for anything that is beyond the given uses, they have violated this term. Or, if interpreted broadly, the word "primarily" might be understood to mean that at least one of the listed uses was accomplished in any indirect way.

This ambiguity chills research because researchers know that there is a possibility of liability if the term is read narrowly to exclude related activities like publication of results. To avoid that possible liability, researchers may be more circumspect in releasing publications on vulnerabilities, including them in academic tenure files, presenting on them at conferences, or other ancillary activities.

The limitation's requirement that information about a computer program's vulnerabilities be used 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" also adversely effects researchers. This is because the limitation raises the possibility that using the information about a vulnerability to dissuade consumers from using a vulnerable device that cannot be made safe or secure because the vulnerability cannot be fixed, or because the device's vendor refuses to fix the vulnerability. While doing so is arguably aimed at improving the security of "those who use" the device, that language might also be read to not apply where disclosure is aimed at ensuring that *no one* uses a device because it is inherently unsafe and/or insecure. This limitation accordingly chills researchers from

[135] *See* 17 U.S.C. § 1201 (a)(1)(B).

[136] 37 C.F.R. 201.40(a)(7)(ii).

addressing and publicizing particularly egregious vulnerabilities that are most in need of public disclosure.

Finally, the Use Limitation adversely affects noninfringing research because it conditions eligibility for the exemption on the behavior of people other than the circumventor. That is, it makes the circumventor liable if someone else uses the information they derived to commit copyright infringement. Just as a theater critic cannot prevent a person from reusing fairly used snippets in a critique of a play in a non-fair, infringing context, a researcher cannot ultimately prevent a third-party from using the noninfringing information for an infringing use. The Office cannot condition eligibility for an exemption based on the future behavior of a third party with whom a researcher may have no direct relationship, much less the right or ability to control.

Because the Use Limitation adversely affects noninfringing research, the Office should remove it.

b. The 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

v. Such other factors as the Librarian considers appropriate.[137]

Each of these factors weigh in favor of granting the proposed modifications.

The availability of copyrighted works. In 2015, the Register found that this first statutory factor favors proponents of a general good-faith security research exemption.[138] The Register reasoned that the "more salient consideration" in this factor is "whether there will be greater availability of copyrighted works in general if an exemption is granted."[139] The Register found that opponents of a general good-faith security research exemption did not establish that such an exemption would have a negative impact on the availability of copyrighted works.[140] Rather, the Register found that proponents of such an exemption had "persuasively establish[ed] that an exemption could increase the availability of works based

[137] 17 U.S.C. § 1201(a)(1)(C).

[138] 2015 Recommendation at 310.

[139] *Id.*

[140] *Id.*

on security research, such as scholarly articles and presentations, as well as new computer programs aimed at rectifying discovered flaws."[141]

The existing good-faith security exemption is limited to narrowly defined classes of works, placing many works researchers wish to study outside of the scope of the exemption.[142] A good-faith security research exemption without limitations will increase the number of copyrighted works available for study by expanding the existing narrowly-defined good-faith security research exemption.[143] Security researchers will make use of access to this broader class of works to further advance the safety and security of software and devices. Furthermore, the works themselves may become more useful and more valuable through this increased safety and security.[144]

The availability for use of works for nonprofit archival, preservation, and educational purposes. In 2015, the Register determined that this factor weighs in favor of a good-faith security research exemption.[145] The Register determined that "an exemption for good-faith security research is likely to increase the use of works in educational settings."[146] Further, the Register noted 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."[147]

Here the analysis is the same as in 2015, and this factor weighs in favor of granting the petition's modifications because removing the limitations will increase the use of works in an educational setting. The current exemption introduces a risk of liability for students and teachers because it is ambiguous as to exactly what activities are allowed.[148] The majority of research and scholarship is conducted by academic researchers in educational settings and so these ambiguities hinder student involvement because teachers are far less likely to involve students when those students may be exposed to individual liability.[149] A broad exemption would also increase educational access, and improve the educational opportunities available for budding security researchers. The five limitations that we wish to remove adversely affect information security research.[150]

[141] *Id.*

[142] *See* discussion *supra*, Part E(3)(a) (Device Limitation).

[143] *Id.*

[144] *See* discussion *supra*, Part (E)(2)(c) (effect on the relevant market).

[145] 2015 Recommendation at 310.

[146] *Id.*

[147] *Id.*

[148] *See* discussion *infra*, Documentary Evidence (Felten and Halderman Personal Statement).

[149] *See* discussion *infra*, Documentary Evidence (Felten and Halderman Personal Statement).

[150] *See* discussion *supra*, Part (C) (Overview); *see also* discussion *supra*, Part (E)(3)(a) (the current exemption's limitations have significant adverse effects on noninfringing security research).

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. In the 2015 proceeding, the Register found that this factor "weighs strongly in favor" of the good-faith security research exemption.[151] The Register determined that the 2015 record established that a good-faith security research "will enhance criticism, comment, news reporting, teaching, scholarship and research."[152] Following the reasoning in the second statutory factor, above, the Register found that teaching and scholarship are enhanced by a good-faith security research exemption.[153] The Register found that "research is at the core of the proposed exemption," and that enabling good-faith security research would promote further research.[154] Lastly, the Register found that a good-faith security research exemption could enhance media attention to, and reporting on, software security issues.[155] Thus, the Register found that this factor weighs in favor of enabling good-faith security research.[156]

Using the same analysis here, this factor weighs strongly in favor of granting this petition's modifications because doing so enables good-faith security research. Good faith security research includes criticism, commentary, news reporting, teaching, scholarship, and research. All aspects of security research, from scholarship, to teaching, to testing, to commenting, criticizing, and reporting, are disincentivized by the current limitations and ambiguities in the current exemption.[157] The resulting chilling effects inhibit key security research, hindering the security of critical information infrastructure, including national security.[158]

The effect of circumvention of technological measures on the market for or value of copyrighted works. In 2015, the Register determined that this factor is neutral, or, at most, weighs "marginally in favor of [a security research] exemption."[159] The Register determined that the "effect of the exemption on the market for or value of copyrighted works would generally not be adverse."[160] The Register found the argument that "granting the exemption could erode the public's confidence in the safety and security of products that are found" was flawed.[161] The Office characterized that argument as "not truly a copyright concern"

[151] 2015 Recommendation at 311.

[152] *Id.* at 310.

[153] *Id.* at 310–311.

[154] *Id.* at 311.

[155] *Id.*

[156] *Id.*

[157] *See* discussion *supra,* (E)(3)(b)(ii) (the availability for use of works for nonprofit archival, preservation, and educational purposes).

[158] *See* discussion *infra*, (E)(3)(b) (other factors).

[159] 2015 Recommendation at 311.

[160] *Id.*

[161] *Id.*

because the concern is rooted in the existence of security defects in computer programs "rather than security researchers' access to those programs."[162] The Office further noted that "knowledge of and ability to correct such flaws will in fact enhance the value of the software and products at issue."[163]

This factor also favors granting the proposed modifications. Removing the Device Limitation will allow researchers to investigate on a wide range of devices, but it will not change the analysis regarding the market for the original device. Similarly, removing the Controlled Environment Limitation will expand researchers' ability to research, but will not affect this analysis regarding the market for the original copyrighted work. None of the proposed modifications change the analysis under this factor from the Register's analysis in 2015.

In general, an exemption for security research has a positive net effect on the market for software and devices. While 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.[164] Any damage to the market for copyrighted works will result only from the exposure of inherent shortcomings in the works themselves

Moreover, coordinated disclosure guidelines help to reduce the risk of market impacts by allowing companies time to address vulnerabilities before they are made public. This dynamic will create a stronger incentive for secure works and opportunity to repair deficient technologies. Thus, the net effect of a general exemption will be to increase the quality and value of the works themselves and the safety and security of the consumers who depend on them.

Other factors. The Librarian should consider the scope of its authority, national security, and First Amendment free speech in evaluating these proposed modifications.

The Librarian's scope of inquiry in this rulemaking is limited to copyright infringement concerns. Congress authorized the Librarian to determine "whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition [against circumvention] in their ability to make noninfringing uses."[165] In 2015, the Register determined that good-faith security research is likely to be noninfringing fair use.[166] As demonstrated above, security research is fair use because (i) the purpose and character of the use is for nonprofit, educational purposes, (ii) the underlying copyrighted work is substantially functional, (iii) the amount and substantiality of the

[162] *Id.*

[163] *Id.*

[164] 2015 Recommendation at 311.

[165] 17 U.S.C. § 1201(a)(1)(B).

[166] 2015 Recommendation at 300; *see* discussion *supra,* (E)(2)(c) (non-infringing fair use).

portion used in relation to the entire copyrighted work is negligible, and (iv) research has no effect upon the potential market for the original copyrighted work.[167]

Importantly, Congress did not authorize the Librarian to regulate noninfringing uses. Rather, Congress gave the Librarian the authority to reduce harm to noninfringing uses, which is the opposite of restricting noninfringing uses by regulating them.[168] The analysis should stop after the Register determines good-faith security research is a noninfringing fair use because Congress did not authorize any further analyses.

The Office should follow its own advice regarding the scope of its authority. In 2015, the Register noted that "[t]he rules that should govern [good-faith security] research hardly seem the province of copyright, since the considerations of how safely to encourage such investigation are fairly far afield from copyright's core purpose of promoting the creation and dissemination of creative works. Rather, the rules that should govern are best considered by those responsible for our national security and for regulating the consumer products and services at issue"[169]

The Office, however, introduced several limitations that addressed concerns other than copyright's core purpose of promoting the creation and dissemination of creative works. Specifically, the Office introduced the Controlled Environment Limitation to "avoid harm to individuals or the public," even though issues of public safety are beyond the scope of copyright law and are covered by many other governmental and nongovernmental entities.[170]

The Office also introduced the Device Limitation, arguing that "[a]s Congress made clear in enacting section 1201, the 'particular class of copyrighted works' [is intended to] be a narrow and focused subset of the broad categories of works . . . identified in section 102 of the Copyright Act."[171] We disagree.

Congress did not intend the Office to enact a narrowly construed security research exemption for several reasons:

- First, Congress explicitly showed that it intended a security research exemption by including the security testing permanent exemption, Section 1201(j).[172]
- Second, Congress intended the exemptions to be flexible as shown by its broad delegation to the Office to create new exemptions that would adapt to address any adversely affected noninfringing use under 1201(a). In fact, Congress specified that part of the reason it created the triennial rulemaking procedure scheme was to enable flexibility, recognizing that it could not predict the future of the technological

[167] *See* discussion *supra,* (E)(2)(c) (non-infringing fair use).

[168] 17 U.S.C. § 1201(a)(1)(C).

[169] 2015 Recommendation at 316.

[170] *See id.* at 318.

[171] *Id.* at 317 (emphasis omitted) (quoting H.R. Rep. No. 105-551, pt. 2, at 38 (1998)).

[172] 17 U.S.C. § 1201(j).

landscape.[173] The Office should feel confident to expand the current exemption because by doing so it would directly follow Congressional intent as shown by the exact wording of the DMCA.

The Register also introduced the Access and Use Limitations, which prevent researchers from using the derived information for later publication and for advising the public against using an unsafe device, in order to track the language of the permanent exemptions, even though she also concluded that the underlying research was noninfringing.[174] Introducing these limitations is outside the Register's authority because Congress did not give the Register the authority to regulate non-infringing use.

Finally, the Register introduced the Other Laws Limitation in order to address the concerns of the 2015 proceedings' opponents, as well as the Department of Transportation, the Environmental Protection Agency and the US Food and Drug Administration.[175] This action fell outside the Register's authority because these concerns fall outside the scope of copyright, which is the sole focus of the Register's authority.[176] The Other Laws Limitation chills noninfringing research by imposing additional liability and ambiguity. Thus, in order to avoid overstepping the limited ambit of the inquiry in this proceeding, the Office should grant this petition's modifications that enable an unlimited good-faith security research exemption.

To the extent that the Office does consider the rules that govern good-faith security research, there are many various laws that already govern such research. The CFAA criminalizes accessing many specific types of information on computers without authorization.[177] The CFAA effectively protects the public from bad faith computer hacking by enabling the government to enforce such action with criminal liability. Other laws, such as the USA PATRIOT Act and state and federal criminal codes, also protect the public from bad actors.[178]

In addition to these laws, good-faith security researchers follow strict norms and customs. In the course of research, if a researcher finds insecure or troubling information, that researcher follows norms of responsible disclosure, including informing the host entity of the discovered vulnerability. Researchers also follow ethical norms in the field which

[173] H.R. Rep. No. 105-551, pt. 2, at 36 (1998).

[174] 2015 Recommendation at 318–19, 300; *see also* discussion *supra*, Part E(3)(a) (Access Limitation and Use Limitation).

[175] 2015 Recommendation at 318.

[176] 17 U.S.C. § 1201(a)(1)(C) (authorizing the Register to determine whether "persons who are users of copyrighted work are … adversely affected by the prohibition [against circumvention] in their ability to make noninfringing uses"); *see* 2015 Recommendation at 318 (summarizing the other agencies' concerns).

[177] 18 U.S.C. § 1030.

[178] *See e.g.,* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56.

include obtaining consent from operators of systems where needed to avoid harm to users of those systems—even where receiving permission from the copyright holder in the system's software is impracticable—as well as compliance with computer hacking laws. If any research may include human subjects, researchers follow the Common Rule in order to protect the participants.[179]

Researchers adhere to these customs because entities such as funding agencies and scholarly journals are unlikely to sponsor or to publish research related to projects that do not follow these standards. As a result, good-faith security research does not risk public safety.

It is also worth noting that a bad-faith computer hacker who is trying to cause harm is not likely to be deterred by limitations on the prohibition to circumvent. However, limitations to circumvent do prevent good-faith security researchers from discovering and preventing such attacks.

Good faith security research testing is a matter of national security. Such research is vital to maintaining safe national cybersecurity. DHS explains that as "information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend."[180] Cyber security risk mitigation is the priority of an executive order by President Donald J. Trump; and it is currently the policy of the executive branch to support the growth and sustainment of a workforce skilled in cybersecurity.[181] Additionally, Congress, the National Telecommunications and Information Administration (NTIA), and other government entities support improving cyber and computer security as a national priority, and the Copyright Office can do its part by granting this petitions' modification requests.[182]

The potential harms of a national cybersecurity breach cannot be overestimated. In January 2017, the Central Intelligence Agency, the Federal Bureau of Investigation, and the National Security Agency released a report that showed 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

[179] *See e.g.,* 45 C.F.R. § 46.

[180] *Cybersecurity Overview*, U.S. Dep't of Homeland Security (Sept. 27, 2016), https://www.dhs.gov/cybersecurity-overview.

[181] Exec. Order No. 13,800, 82 Fed. Reg. 22391 (May 16, 2017).

[182] *See e.g.,* Letter from Lawrence E. Strickling, Assistant Sec'y for Commc'ns & Info., Nat'l Telecomms. & Info. Admin., U.S. Dep't of Commerce, to Maria A. Pallante, Register of Copyrights and Dir., U.S. Copyright Office, at 73 (Sept. 18, 2015) (citation omitted); Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015); Angela Simpson, *Improving Cybersecurity Through Enhanced Vulnerability Disclosure*, Nat'l Telecomm. & Info. Admin. (Dec. 15, 2016), https://www.ntia.doc.gov/blog/2016/improving-cybersecurity-through-enhanced-vulnerability-disclosure.

blended "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.'"[183]

Cybersecurity breaches have also resulted in harms stemming from the unauthorized dissemination of consumer data, such as the recent high-profile breach at Equifax, where 143 million American consumers' sensitive personal information was stolen. [184] Breaches involving credit cards and retail consumers have become relatively commonplace.[185] Other important national security concerns that are vulnerable to exploitation by bad-faith hackers include risks to critical infrastructure, essential services, and federal networks.[186]

Security research addresses national cybersecurity concerns by discovering and working to solve computer system vulnerabilities before bad-faith hackers find and exploit those vulnerabilities. Rather than having negative repercussions on the safety and security of critical infrastructure by allowing the malicious exploitation of flaws and vulnerabilities, a broad exemption for security research will help identify and repair such flaws and vulnerabilities before they can be exploited.

Furthermore, promoting security research is vitally important for the government and the economy. The United States has the resources to lead the world in the creation and maintenance of secure software and devices, and a broad, general good-faith security research exemption will promote this goal.

Finally, the conduct and publication of security research is protected by the First Amendment. As a result, granting the proposed modifications is critical, at a bare minimum, to avoid an unconstitutional application of Section 1201. The triennial exemption process is Section 1201's mechanism for recognizing fair use, which the Supreme Court has labeled a "built-in First Amendment accommodation."[187] The constitutionality of the triennial rulemaking process itself is being challenged in pending federal litigation that asserts that the triennial procedure is an unconstitutional speech-licensing regime which fails to pass strict

[183] National Intelligence Council, *Assessing Russian Activities and Intentions in Recent US Elections*, Intelligence Community Assessment (2017) *available at* https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[184] *The Equifax Data Breach: What to Do*, Fed. Trade Commission (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

[185] *See e.g., Breach at Sonic Drive-In May Have Impacted Millions of Credit, Debit Cards*, KrebsonSecurity (Sept. 26, 2017), https://krebsonsecurity.com/2017/09/breach-at-sonic-drive-in-may-have-impacted-millions-of-credit-debit-cards/.

[186] *Cybersecurity*, U.S. Dep't of Homeland Security, https://www.dhs.gov/topic/cybersecurity (last visited Dec. 18, 2017).

[187] *Eldred v. Ashcroft*, 537 U.S. 186, 190 (2003).

scrutiny.[188] The Register agreed in the 2015 Recommendation that "regulating disclosure of vulnerabilities may implicate First Amendment concerns."[189] Thus, failing to grant the proposed modifications would result in unconstitutionally limiting researchers' free speech.

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

Limitations in Section 1201's built-in exemptions and in the existing exemption presumptively renewed by the Office are the cause of adverse effects on information security research because the exemptions are insufficiently clear and lack the breadth to cover the uses in the proposed modification. The lack of clarity in the statutory prohibition on circumvention chills security research. Non-circumventing methods are incapable of achieving the same results as circumvention, especially where circumvention itself is the process security researchers study. In most cases of security research, there are no reasonable alternatives to circumvention. This is because all instances of the software or device under investigation are protected by TPMs, thus no investigation can take place without bypassing a TPM.

In addition, software developers and copyright holders lack adequate incentives to conduct the necessary security research themselves. In many cases, developers and copyright holders attempt to leverage Section 1201 against researchers to *conceal* security vulnerabilities. Notwithstanding the permanent exemptions in Section 1201, the Register has "concluded that the permanent exemptions in sections 1201(f), 1201(g), and 1201(j) are inadequate to accommodate the proposed research activities due to various limitations and conditions contained in those provisions."[190]

The Copyright Office concluded that good-faith security testing has been hindered by TPMs that protect copyrighted programs—specifically, the ability to identify, disclose and correct malfunctions, security flaws and other vulnerabilities.[191] Yet the current exemption is overly-narrow, lacks clarity and excludes other protected uses on circumventing access controls. Specifically, the limitation restricts dissemination of information, authorization requirements, reliance on multifactor tests, and other infirmities to fulfill researchers' desired activities.

Finally, in most cases of security research, there are no reasonable alternatives to circumvention. This is because all instances of the software or device under investigation are protected by TPMs, thus no investigation can take place without bypassing a TPM. In addition, software developers and copyright holders lack adequate incentives to conduct the necessary security research themselves. In many cases, developers and copyright holders

[188] Complaint, para 1 (July 21, 2016) ECF No. 1:16-cv-01492-EGS; *see also Green v. U.S. Department of Justice*, Electronic Frontier Found, https://www.eff.org/cases/green-v-us-department-justice (last visited, Dec. 17, 2017).

[189] 2015 Recommendation at 311.

[190] 2015 Final Rule, 80 Fed. Reg. at 65,956.

[191] 2015 Recommendation at 305 (internal citations omitted).

attempt to leverage Section 1201 against researchers to *conceal* security vulnerabilities rather than fixing them.

*   *   *

For the foregoing reasons, the Librarian should grant the proposed modifications.

Respectfully submitted,

/s/

Blake E. Reid
Elizabeth Field
Justin Manusov

Documentary Evidence: Personal Statement

The following documentary evidence is a personal statement about the importance of granting these modifications composed by Professors Felten and Halderman.

I, Ed Felten, am a Professor of Computer Science and Public Affairs at Princeton University and the Director of Princeton's Center for Information Technology Policy. My primary academic interests include software security, Internet security, electronic voting, cybersecurity policy, technology for government transparency, network neutrality and Internet policy. Prior to my current position at Princeton, I was the Chief Technologist for the U.S. Federal Trade Commission and was named the Deputy U.S. Chief Technology Officer in 2015.

I, Alex Halderman, am a Professor of Computer Science and Engineering at University of Michigan and the Director of University of Michigan's Center for Computer Security and Society. My primary academic interests include software security, network security, data privacy, anonymity, electronic voting, censorship resistance, computer forensics, ethics, and cybercrime.

Introduction

We have conducted extensive research aimed at improving the security and robustness of information systems. Throughout the course of our research, we have investigated systems to discover security flaws and vulnerabilities in software devices and engage in scholarship through publications and academic conferences. The primary aims of this research include improving technology and protecting consumers.

In order for good-faith security researchers to secure modern information systems from attack, a researcher must first *understand* the weaknesses that make the systems vulnerable. The main challenge in their work is that both products and attack techniques evolve constantly. To gain understanding, academic and industry security researchers must examine deployed software and devices to determine which vulnerabilities are present, and to gain insight into how these vulnerabilities may be exploited by motivated bad faith attackers.

Unfortunately, the process of examining real systems carries potential legal risks, many of which result from Section 1201 and the limitations in the current security research exemption. In fact, the limits and ambiguities in the current exemption have become larger than life in the research community to the extent that researchers often avoid activities that are likely accepted uses because they fear personal liability. Researchers might not have access to attorneys, and without legal advice, they often decide that the risk of personal liability is so great that they avoid any circumvention behavior entirely.

In support of our request for modification of the current security research exemption, this document explains why removing the current limitations is essential to enabling our consumer-protective research. Specifically, and in addition to the material laid out in the comment, we address the Device Limitation, the Controlled Environment Limitation, the Access Limitation, and the Use Limitation.

Device Limitation

The Device Limitation, which requires that circumvention be undertaken only on specific categories of devices, severely restricts our research because it is ambiguous and it is limiting.

The main category of device that is ambiguous is consumer devices. The Office is silent as to what a consumer device is. Because this term is not defined, we do not know whether it will be interpreted narrowly, to mean any device that a consumer individually owns and uses, such as a personal computer, or if it will be interpreted broadly to incorporate any device that a consumer even indirectly comes in contact with. This uncertainty chills our research because we are less likely to take on projects that may fall outside the scope of a narrowly construed "consumer device" to avoid potential liability.

Furthermore, this limitation directly chills our ability to teach effectively, given that most academic research projects require the assistance of graduate students who would also be at risk of liability. Though we, as academic researchers, may feel comfortable taking a limited amount of risk, there are ethical challenges in exposing students to the same risk. We support a broad interpretation of consumer devices, but without a clear definition from the Copyright Office, we support removing the categories of devices altogether.

There are several important research projects that are too risky to undertake because the consumer device category is ambiguous. These examples fit the broad definition of consumer device, in that they are systems that are indirectly used by consumers:

- **Building automation systems**. A building automation system is the automatic centralized control of a building's heating, ventilation and air conditions, lighting and other systems. A building automation system is not bought or owned directly by consumers. However, it is relied upon and benefits consumers every time they enter such a building.
- **Commercial networking equipment**. Networking equipment is the physical infrastructure, such as routers, switches, and firewalls, that facilitates communication on computer networks. Businesses and Internet service providers operate specialized network equipment. However, consumers rely on this equipment indirectly whenever they send data over the Internet or interact with computer servers operated at a business.
- **Traffic control systems**. These systems include the computers, sensors, and networks that control traffic lights and electronic road signs. These systems are not available for individual consumer purchase. However, consumers rely heavily on traffic systems functioning properly.

Importantly, we note here that norms and customs of academic research require that we only attempt to exploit vulnerabilities in these systems with the prior permission of the owner—though not the holder of copyright in the software in the system—and we conduct any investigation into such systems in ways that would not cause risk or harm to any person.

It is very important to be able to analyze the security of these types of systems in order to protect consumers by ensuring that bad faith actors cannot attack and manipulate the system. But because these systems may fall outside a narrow interpretation of consumer devices, we would undertake significant risk of liability by researching them.

Controlled Environment Limitation

The Controlled Environment Limitation, which requires that circumvention be undertaken only in a controlled environment, severely restricts our research because it is ambiguous and it is limiting.

This limitation is ambiguous because it does not define what a controlled environment is. In computer security research, some research is conducted entirely within a laboratory and simulated environment. However, the aim of security research is to identify potential vulnerabilities, and this process often needs to include situations where some variables are unknown. Because the controlled environment limitation is unclear as to what a controlled environment is, we often avoid necessary research that may implicate unknown aspects.

There are many examples of research that is risky due to the ambiguity of the Controlled Environment Limitation. Computer security research often includes Internet-wide scanning. Internet-wide scanning involves making small numbers of harmless connection attempts to publicly accessible computers. This allows researchers to measure the global Internet and analyze trends in technological deployment and security. Internet-wide scanning may also consist of standard connection attempts followed by RFC-compliant protocol handshakes with responsive hosts. The data connected through these connections would consist solely of information that is publicly available on the Internet.

This limitation should also be removed because it prevents us from researching in the field, where the environment is purposefully uncontrolled. The aim of security research is often to observe how a system interacts with a live and unpredictable environment. Consumers rely on systems being secure in the real-world environment. In order to most accurately investigate whether systems are secure, we must be able to work on systems in real-world environments. Research in uncontrolled environments allows us to measure variations caused by undetected sources, clarify causation from correlation, improve reliability, and perform verification.

Importantly, this type of research does not include research that would risk human injury or harm. As mentioned above, researchers follow strict norms and customs that protect against such harms, and academic research that involves human subjects is tightly regulated under the Common Rule.

There are several examples that demonstrate the type of research that needs to be done in uncontrolled environments. One such example is passive monitoring. Passive monitoring is a method of collecting data from systems without interfering with the operations of that system. Passive monitoring allows us to gather information about how a system works without changing anything about the system. Some examples of passive monitoring that would be useful to conduct include collecting data on how messages exchanged by smart vehicles or Internet of Things devices are encrypted. Monitoring the encrypted traffic of a large sample of different kinds of devices in their real-world configurations would likely reveal flaws in some of the devices that would allow attackers to decrypt the messages and attack the underlying systems.

Other examples of uncontrolled environments include the previously-mentioned building automation systems that control heating, ventilation, and other systems. In order to protect against malicious interferences, security researchers need to be able to research such systems. However, it is impossible to bring a building automation system into the controlled environment of a lab. Furthermore, a researcher would want to investigate the building automation system specifically in the real-world environment in order to observe things like whether a passerby's phone interferes with the system and whether weather changes effect system operation. These possible interferences are unpredictable, yet essential to ensuring the system operates securely in the real world.

An important final example of research that needs to be done in a real-world environment is ensuring that electronic voting machines are secure in live conditions. Again, and very importantly, this does not mean that researchers would research or interfere with electronic voting machines while citizens are voting in an election. Rather, it means that researchers, in order to ensure that no bad actor can interfere with elections, need to be able to ensure and demonstrate that electronic voting machines are not "hackable" in the real-world environment. Currently, we can only test these machines in laboratory conditions without risking potential liability.

By freeing researchers from the burden of controlling every variable in scientific experimentation, the Copyright Office will allow us to observe unanticipated variables and confounding factors. The Controlled Environment Limitation significantly chills our security research because it is prohibitively difficult to ensure that all aspects of an environment are controlled.

Furthermore, similar to the above Device Limitation, this limitation directly chills our ability to teach effectively, given that most academic research projects require the assistance of graduate students who would also be at risk of liability. Again, while we, as academic researchers, may feel comfortable taking a limited amount of risk in a project that includes an arguably uncontrolled environment, there are ethical challenges in exposing students to the same risk.

Access Limitation and Use Limitation

The Access and Use Limitations should be removed because they are ambiguous as to whether we may use the post-circumvention information in academic writings, at academic conferences, or for teaching in the classroom. New academic research and discovery in any field is grounded upon the existing body of knowledge in that field. This body of knowledge is made up in large part by academic peer-reviewed publications and expanded upon by academic lectures and conferences.

Computer security is a fast-evolving field. As computer security researchers gather new insights, we need to be able to disseminate the new information to other researchers in order to advance the field of security research. Furthermore, we need to able to speak freely to the general public about our findings to best protect consumers from systems that may be extremely vulnerable.

Currently, the security research exemption allows us to use the information we discover "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." This language should be removed because it does not allow researchers to recommend that the public stop using a particular system altogether. Sometimes in security research, we find that the security vulnerability is so fundamental to the operation of the system that it is impractical to try to fix the vulnerability because doing so might involve rewriting the entire program from scratch. When this situation arises, we need to be able to inform consumers that the system is insecure so they can protect themselves by stopping using the program altogether.

Removing the Access and Use Limitation is essential because doing so will allow us to publish and speak freely about our research without fear of liability.