UNITED STATES COPYRIGHT OFFICE

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

**Reply Comments on Proposed Class 10**
**Computer Programs—Security Research**

of

**Prof. Ed Felten**
**Prof. J. Alex Halderman**
**Center for Democracy & Technology (CDT)**

*Representatives*

**Samuelson-Glushko Technology Law & Policy Clinic**

Colorado Law

*Counsel to Prof. Felten and Prof. Halderman*

Blake E. Reid, Director

Brett Hildebrand and Alex Kimata,
Student Attorneys

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

**Center for Democracy and Technology**

Stan Adams, Policy Counsel
sadams@cdt.org

Maurice Turner, Senior Technologist
mturner@cdt.org

Ferras Vinh, Policy Counsel
fvinh@cdt.org

202-637-9800
1401 K Street NW
Suite 200
Washington, DC 20005

## Table of Contents

## Discussion

Prof. Felten, Prof. Halderman and the Center for Democracy & Technology (CDT) respectfully submit these reply comments in response to comments in favor of and objections to modifications that would remove several limitations from the proposed Class 10 exemption of good-faith security research from the anti-circumvention provisions of Section 1201 of the Digital Millennium Copyright Act (DMCA).[1]

Proposed Class 10 includes:

> (i) Computer programs, where the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates solely for the purpose of good-faith security research and does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986, as amended and codified in title 18, United States Code; and provided, however, that, except as to voting machines, such circumvention is initiated no earlier than 12 months after the effective date of this regulation[2], and the device or machine is one of the following:
>
> (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.
>
> (ii) For purposes of this exemption, "good-faith security research" means accessing a computer program solely for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability, where such activity is carried out in a controlled environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those

[1] Library of Congress, Copyright Office, Notice of Proposed Rulemaking, Exemptions to Permit Circumventions of Access Controls on Copyrighted Works, 82 Fed. Reg. 49,550, 49,555 (Oct. 26, 2017) ("NPRM").

[2] In addition to presumptively renewing the exemption, the Office noted that the delay in the existing version of the regulation will be removed. *Id.* at 49,555 & n.50.

> who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement.[3]

In their initial comments, Prof. Halderman and Prof. Felten explained that five limitations in the presumptively renewed security research exemption adversely affected their ability to make noninfringing uses of computer software in the context of good-faith security research:[4]

1. The *Device Limitation*, which limits the exemption to three types of devices or machines: a device or machine primarily designed for use by individual consumers (including voting machines), a motorized land vehicle, and 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 for patient care;[5]
2. The *Controlled Environment Limitation,* which limits the exemption to security research which is "carried out in a controlled environment designed to avoid any harm to individuals or the public";[6]
3. The *Other Laws Limitation*, which requires that good-faith security research is undertaken on a "lawfully acquired device or machine on which the computer program operates" and does "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";[7]
4. The *Access Limitation*, which limits the exemption to research "solely for the purpose of good-faith security research" and that limits good-faith security research to accessing a computer program "solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability;"[8]
5. The *Use Limitation*, which requires "information derived from" exempted security research to be "used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those that use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement."[9]

[3] 37 C.F.R. § 201.40(b)(7).

[4] Comments of Profs. Felten and Halderman, (Dec. 19, 2017), https://www.copyright.gov/1201/2018/comments-121817/class10/class-10-initialcomments-felten-halderman.pdf ("Felten Halderman Initial Comments").

[5] 37 C.F.R. § 201.40(b)(7).

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] *Id.*

Prof. Halderman, Prof. Felten, and CDT urged the Office to remove these limitations from the exemption in their petitions at the start of this rulemaking.[10] Several parties opposed the removal of the limitations.[11] Although CDT and Professors Felten and Halderman filed separate petitions in response to the Office's Notice of Inquiry and separate comments in response to the Office's Notice of Proposed Rulemaking, Prof. Felten, Prof. Halderman, and CDT agree that there are significant and similar problems with current limitations in the Security Research exemption and that the record strongly supports eliminating them. We therefore submit these joint reply comments.

The record established in this proceeding strongly demonstrates that the Office should remove the limitations. Removal of each of the limitations is strongly supported by a range of stakeholders, while the issues raised by objectors are largely attenuated from the copyright considerations that are relevant to this proceeding.

## I. The record supports removing the Device Limitation.

The current exemption for security research limits security researchers to only three classes of devices on which to conduct their research:

(1) Devices or machines primarily designed for use by individual consumers (including voting machines);[12]

(2) Motorized land vehicles; and

(3) Medical devices designed for whole or partial implantation in patients or corresponding personal monitoring systems that are not and will not be used by patients or for patient care.[13]

[10] Petition of Prof. Ed Felten and Prof J. Alex Halderman (Sept. 13, 2017), https://www.copyright.gov/1201/2018/petitions-091317/class10/class-10-newpetition-felten-halderman.pdf.; Petition of CDT (Sept. 13, 2017), www.copyright.gov/1201/2018/petitions-091317/class10/class-10-newpetition-cdt.pdf.

[11] Comments of the Auto Alliance, the Software and Information Industry Association (SIIA), The Business Software Alliance (BSA), The App Association, Joint Creators (Motion Picture Association of America, Inc., the Entertainment Software Association, the Recording Industry Association of America, and the Association of American Publishers), the Election System Providers (ESP), DVD Copy Control Association (DVD CCA) and the Advanced Access Content System Licensing Administrators, LLC (AACS LA), Secretary of State of North Dakota, and National Association of Secretaries of State (NASS).

[12] We understand that election officials, staff, and volunteers are "individual consumers" and thus that voting machine systems encompass scanners, tabulators, and poll books within the "primarily designed for use by individual consumer" limitation. *But see* Comments of Election Systems Providers at 3 (Feb. 13, 2018), https://www.regulations.gov/document?D=COLC-2017-0007-0138 ("ESP Comments").

[13] 37 C.F.R. § 201.40(b)(7)(i)(A-C).

Prof. Felten and Prof. Halderman noted in their initial comments that the Device Limitation chills security researchers because its scope is ambiguous.[14] There are two primary problems with the limitation:

1. The "primarily designed for" language is textually ambiguous and amenable to different interpretations. "A narrow interpretation might inquire into a developer's state of mind in creating a particular device. On the other hand, a broader interpretation might focus objectively on whether a device is indeed used by consumers regardless of developer's intent."[15]
2. The current exemption offers no explanation of what "use by individual consumers" means. It remains unclear whether this language 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 directly uses or is a part of a larger system that a consumer interacts with.[16]

These uncertainties chill 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.[17]

The Device Limitation is included in the current exemption only because the Register in the Sixth Triennial proceeding concluded in the previous triennial rulemaking that the record did not support categories of devices beyond those included in the Limitation.[18] Thus, in that proceeding the Register confined the Device Limitation to those devices.

While we disagree with the Register's 2015 conclusion, the concern that underpinned the inclusion of the Device Limitation in that proceeding has been obviated by the significant support in this proceeding for removing this Limitation. Indeed, multiple commenters explained in detail how software embodied in devices potentially outside the categories currently covered in the Device Limitation contain or are likely to contain vulnerabilities similar to those found in devices included in the existing categories.[19] More specifically:

[14] Felten Halderman Initial Comments at 18.

[15] *Id.*

[16] *Id.* at 19.

[17] *Id.* at 19.

[18] United States Copyright Office, Section 1201 Rulemaking: Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendations of the Register of Copyrights (October 2015) at 317 ("2015 Register's Recommendations").

[19] Comments of Center for Democracy & Technology, at 2-6, 18-21 (Dec. 19, 2017), https://www.regulations.gov/document?D=COLC-2017-0007-0075 ("CDT Initial Comments"); Comments of the United States Association of Computing Machinery (Dec. 19, 2017), https://www.regulations.gov/document?D=COLC-2017-0007-0096 ("USACM

- Prof. Felten and Prof. Halderman explain that the Device Limitation chills noninfringing research and inhibits the discovery of vulnerabilities in software of many important devices because the definition of consumer device is ambiguous and because the Device Limitation prevents researchers from security research on devices not included on the list.[20]
- CDT's comment explains that the limitation potentially excludes "other types of devices that increasingly include software and will also feature security flaws and vulnerabilities, like infrastructure and industrial equipment."[21] Moreover, CDT notes that because software is integrated in a wide variety of different products and physical world processes, "these flaws pose risks that are qualitatively different from the risks associated with traditional security defects confined to the digital environment."[22] Thus, "the exemption should cover a broad range of devices; product-by-product exemptions would make little sense in a world where harmful flaws may exist in any of a wide variety of products or systems" and waiting every three years to include new devices carries significant lag time for researching and discovering new vulnerabilities.[23] For example, researchers have sought to evaluate and ensure the security of encryption modules for financial transactions like ATM withdrawals, toll collection, and infrastructure that communicates with computerized vehicles, which might not be covered under this exemption.[24]
- The Public Policy Council for the Association for Computing Machinery (USACM), the world's oldest and largest membership society for technology and computing professionals, notes that the Device Limitation currently in place "leaves out emerging security threats to systems outside of this scope, such as commercial drones and building environment and physical security systems."[25] Instead the USACM suggests that "[t]here is no reason to enumerate specific categories at all, given that software technology and internet connectivity are increasingly ubiquitous, and it's difficult to know exactly what new threats may arise."[26]
- The Free Software Foundation (FSF) also notes the Device Limitation does not make sense within this security research exemption because "[t]he need to

Comments"); Comments of Prof. Matt Green, at 1-2 (Dec. 19, 2017), https://www.regulations.gov/document?D=COLC-2017-0007-0100 ("Green Comments").

[20] Felten Halderman Initial Comments at 5, 20-21.

[21] CDT Initial Comments at 1.

[22] *Id.*

[23] *Id.*

[24] *Id.* at 3.

[25] USACM Comments.

[26] *Id.*

understand and improve the security of software and devices does not depend on what the particular software or device is."[27] Furthermore, FSF explains that the current Device Limitation does not protect devices from attacks, but rather furthers attacks on those devices that are not currently included. This is because "[l]imiting the exemption to particular uses provides a guidebook to criminal elements as to what software and devices they can attack without fear of security researchers discovering their methods.[28]

- Prof. Green argued that the Device Limitation has already had an adverse impact on his ability to do security research.[29] In the fall of 2015, he performed "a limited analysis on one of the subjects of his research" which limited his ability to understand and fix potential vulnerabilities within the system precisely because of the Device Limitation.[30] Moreover, Prof. Green notes that he would like to research industrial-grade firewall and private network modules, hardware encryption devices, toll collection systems, non-implantable medical devices, and wireless communication systems that connect vehicles to one another and to the surrounding infrastructure, but is prevented by the device limitation.[31]

No commenters significantly contradict the record's support for removing the device limitation. Therefore, the Register's previous reasoning for recommending the limitation, which hinged exclusively on what the Register perceived as a lack of support, is no longer operative. As a result, the Register must recommend eliminating the Limitation.

Nevertheless, opponents raised objections that primarily fall into three categories:

1. That research on devices outside the categories in the current limitation would be infringing;
2. That eliminating the Device Limitation would create an impermissibly overbroad class; and
3. That eliminating the Device Limitation would endanger the public and cause national security concerns.

While we address each of these arguments on their own merits below, we note at the outset that none of them were pertinent to the Register's justification for including the Device Limitation, which was *solely* based on what the Register perceived as a lack of record support. In particular, the Register expressed no concerns that research on devices outside the categories in the Limitation would give rise to infringement, that the Limitation was included to satisfy Section 1201's scoping requirements, or that the Limitation was included to address safety or security concerns.

[27] Comments of Free Software Foundation, at 2 (Dec. 19, 2017), https://www.regulations.gov/document?D=COLC-2017-0007-0131 ("FSF Comments").

[28] *Id.*

[29] Green Comments at 1-2.

[30] *Id.*

[31] *Id.*

By raising these arguments now, opponents attempt to relitigate issues that the Register resolved in 2015. **The Office should reject this attempt and remove the Device Limitation from the final exemption without regard to these arguments.** Nevertheless, each of these arguments, even if properly considered here, fails on its own merits.

### A. Eliminating the Device Limitation would not permit infringing research.

Some opponents argue that the modification of the exemption to permit security research on devices not already exempted would create uses that are infringing. The Election Service Providers (ESP) object most broadly, arguing that expanding the exemption beyond the existing categories would raise questions of infringement, particularly in the context of election software.[32] They argue that extending the exemption to all forms of election software, including election management software, voter registration software, ballot assembly software, electronic poll book software, tabulation software, and absentee voting software may allow significant infringing activity.[33]

More specifically, ESP argue that election software licenses typically prohibit purchasers from allowing third-party access to the licensed software.[34] Thus, in most cases, ESP allege, any copying of the software would be an infringing license violation and that a state or government who has authority to use the software cannot give a third party a copy of the software without violating 17 U.S.C § 106(1) and (3).[35]

However, modifying the category of devices covered by the security research exemption does not alter the conclusion that security research is a non-infringing fair use. As we explained in significant detail in our initial comments, security research on computer software is a fair use whose non-infringing nature does not depend significantly on the category of device in which the software is embedded.[36] This conclusion is consistent with the Register's Recommendation, which did not rest the inclusion of the Device Limitation on the prospect that security research on software embodied in other devices might be infringing. [37] Furthermore, the Register's analysis concluding that security research was fair use relied on the conclusion that security research was transformative, largely functional in nature, that the copying of the work was necessary and thus consistent with fair use and that the effect on the market would be minimal. [38] None of these conclusions were device specific and they would still apply without the Device Limitation.[39]

[32] ESP Comments at 17-20.

[33] *Id.* at 17.

[34] ESP Comments at 10, 17.

[35] *Id.* at 18.

[36] Felten Halderman Initial Comments at 12-17; CDT Initial Comments at 2.

[37] 2015 Register's Recommendations at 317.

[38] 2015 Register's Recommendations at 300-03.

[39] *See id.*

ESP do not significantly grapple with or attempt to rebut this obvious conclusion, nor do ESP otherwise coherently explain why fair, non-infringing security research on software embodied in devices covered under the Device Limitation would suddenly become infringing if performed on software embedded in a different class of device.

Instead, ESP cursorily contend that security research on a broader range of election software would not constitute fair use:[40]

- Under the first fair use factor, purpose and character of use, ESP argue that while the Register in 2015 concluded there may be "academic inquiry" or "education" in that security research, that conclusion would not apply to other devices.[41] They argue that use by a researcher is not transformative because obtaining an infringing piece of software from the state or downloading a copy is not transformative.[42]
- Under the second fair use factor, the nature of copyrighted work, ESP argue that the Register's conclusion that software on devices is "largely functional in nature"[43] does not apply because the new class of software is broader and more varied, implicating more expressive content and deserving more copyright protection.
- Under the third fair use factor, amount and substantiality, ESP argue that the Register concluded the third factor weighed against a finding of fair use because the Register found "proposed uses would involve reproductions of copyrighted computer programs in their entirety."[44]
- Under the fourth fair use factor, the effect on the market, ESP argue that "acquiring infringing software without paying the customary price is a classic market harm" and that allowing access to unknown security researchers would "greatly increase the risk of piracy of such software."[45] Moreover, they argue that vulnerabilities and criticism of such software will chill demand for their software.[46]

These arguments are unavailing. First, as Prof. Felten and Prof. Halderman explained in detail in their initial comments, engaging in security research and discovering vulnerabilities

[40] ESP Comments at 19.

[41] *Id.* at 18.

[42] *Id.* at 19.

[43] 2015 Register's Recommendations at 301.

[44] ESP Comments at 20 (citing 2015 Register's Recommendations at 301); but see 17 U.S.C. § 117 ("Notwithstanding the provisions of section 106, 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 computer program . . . ."

[45] *Id.*

[46] *Id.*

means that security researchers engage in scholarship, research, criticism, commentary, news reporting, teaching, and/or education that strongly weighs the first factor in favor of fair use.[47] As the Register found in 2015, "[t]he desired research activities may result in criticism or comment about the work and devices in which it is incorporated, including potential flaws and vulnerabilities."[48] The Register also found that "in many cases, research activities may also extend to evaluating and describing how to fix flaws that have been discovered."[49] Thus, the Register concluded that the use was likely to be transformative and that the first factor favored fair use.[50]

Second, contrary to ESP's cursory contention, election software—and most other device-control software—is highly functional and non-expressive, strongly weighing the second factor in favor of fair use.[51] Election software is created primarily to help run elections, a ministerial process of collecting ordered data whose parameters are largely dictated by state and federal constitutions, statutes, and regulations rather than creative or aesthetic considerations. As the Register concluded, "[w]hen a computer program is being used to operate a device, the work is likely largely functional in nature."[52]

Third, the ultimate products of security research do not contain significant portions of the original copyrighted work, thereby weighing the third factor in favor of fair use.[53] Although research may involve transitory or ephemeral copying of entire works, the Register acknowledged that "[c]ourts have been willing to permit complete copying of original work [ ] where it is necessary to accomplish a transformative purpose."[54] The Register has previously concluded that such copying is consistent with fair use.[55]

Finally, ESP concerns about piracy are wildly speculative and unsupported by any evidence that security research would lead to copying. ESP appear primarily concerned that acquisition of their software by security researchers will reveal significant security flaws that will harm the market for their devices. But as Prof. Halderman's and Prof. Felten's initial comment explained in detail, it is a long-standing tenet of copyright and First Amendment jurisprudence that there is no protectable market for criticism or commentary of a copyrighted work.[56] As the Register has acknowledged, the Supreme Court in *Campbell v. Acuff-Rose Music, Inc.*explicitly held that "there is no protectable derivative market for

[47] Felten Halderman Initial Comments at 28.

[48] 2015 Register's Recommendations at 300.

[49] *Id.*

[50] *Id.*

[51] Felten Halderman Initial Comments at 15.

[52] 2015 Register's Recommendations at 301.

[53] Felten Halderman Initial Comments at 16.

[54] 2015 Register's Recommendations at 301.

[55] *Id.*

[56] Felten Halderman Initial Comments at 16 (quoting the 2015 Register's Recommendations at 301).

criticism."[57] While a computer program or software company might suffer economic or reputational harm from the disclosure of its products' security flaws or vulnerabilities, that harm is irrelevant since it does not usurp the original market.[58] And, as Prof. Halderman and Prof. Felten explained, possible economic 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."[59]

Thus, it is universally likely that computer research is non-infringing fair use and that even taking into account the unique arguments of ESP, election software still falls within fair use by security researchers..

ESP nevertheless cursorily argue that Section 117 does not immunize security research because the statute requires the person acting pursuant to it to be "the owner of a copy" of the software and that, because election software is licensed rather than sold, the state and local governments do not own the software nor do the license agreements allow other parties to access the software.[60] Likewise, SIIA disputes that some computer programs (or elements of computer programs) are unlikely to be eligible for copyright protection because they contain functional elements.[61]

As Prof. Felten's and Prof. Halderman's initial comments explain, Section 117 is likely to immunize security research directly in many cases, and there may be cases where elements of the object of research are simply not copyrighted.[62] But even where those considerations are not at play, security research remains a non-infringing fair use. As a result, concerns about infringement provide no basis for the Register to recommend maintaining the device exemption.

### B. The current proposed class is properly tailored to address harms and falls within the Register's authority to create this scope of class.

Some opponents contend that eliminating the Device Limitation for security research would create an overbroad class inconsistent with the Register's authority to promulgate exemptions under Section 1201.[63] More specifically:

[57] 2015 Register's Recommendations at 301 (quoting Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 590 (1994)).

[58] *Id.*

[59] Felten Halderman Initial Comments at 17.

[60] ESP Comments at 18.

[61] SIIA Comments at 3-4.

[62] Felten Halderman Initial Comments at 10-11.

[63] 17 U.S.C. § 1201(a)(1)(C).

- SIIA acknowledges that a class of user may help define a class of work, but argues that other factors must narrow the class, and a lack of such narrowing in this case means the exemption exceeds the scope of the Register's statutory authority.[64]
- Joint Creators argue that eliminating the Device Limitation would take a "broad-stroke approach" that would be "an impermissible, use-based exemption, rather than an exemption for a 'particular class of copyrighted works.'"[65]
- Joint Creators also argue that modifying the exemption would put at "risk every corporate database through which consumers obtain online information or acquire content."[66] This, they argue, was expressly excluded by the Register in 2015 and thus inclusion here would be explicitly against the Register's intent.[67]
- BSA argues that the removal of the Device Limitation would render the 2015 Exemption "inconsistent with the DMCA's requirement that exemptions relate" to a narrow and focused subset.[68]
- ESP argue that the Register has previously rejected this "open-ended" exemption. Instead, they argue that this class of works should be a narrow and focused subset of the broad categories of copyrighted works."[69]
- App Association argues that the DMCA "instructs that exempted classes should 'be a narrow and focused subset of the broad category of works.'"[70]

However, removing the Device Limitation would leave in place a sufficiently narrow and limited class. In her Recommendation, the Register included the Device Limitation in the exemption only because she concluded that the record did not support granting a more

[64] Comments of Software and Information Industry Association, at 3 (Feb. 13, 2018), https://www.regulations.gov/document?D=COLC-2017-0007-0159 ("SIIA Comments").
[65] Comments of Joint Creators, at 4-5 (Feb. 13, 2018), https://www.regulations.gov/document?D=COLC-2017-0007-0167 (arguing that the Register has previously rejected broad proposed categories such "fair use works" or "educational fair use works") ("Joint Creators Comments").
[66] Joint Creators Comments at 6-7.
[67] *Id.* Joint Creators also argue that incidental access to other works ancillary to computer software in the course of performing good faith security research should not be included. *Id.* at 12. It is our understanding that this incidental access is covered under the existing exemption for which the Register has provisionally recommended renewal and urge the Office to reject the Joint Creators' attempt to relitigate this issue.
[68] Comments of (BSA) The Business Software Alliance, at 5 (Feb. 13, 2018), https://www.regulations.gov/document?D=COLC-2017-0007-0147 ("BSA Comments").
[69] ESP Comments at 17.
[70] Comments of App Association, at 3 (Feb. 13, 2018), https://www.regulations.gov/document?D=COLC-2017-0007-0165 ("App Association Comments").

broadly-defined exemption.[71] There was no indication in the Register's reasoning that the inclusion of the Limitation was related to Section 1201's breadth requirements or that, with more factual support, a broader class could not be granted.

Because the record in this proceeding provides evidence that research on other software faces adverse effects because of the anti-circumvention measures and meets the other requirements necessary for the Librarian to expand the classes of software within the exemption, eliminating the Device Limitation would not create an overbroad class. As described *supra*, multiple commenters have noted that things like automated teller machines, toll collections, and building environments fall outside of the Device Limitation, but still experience security problems to those devices that are included.[72]

Moreover, eliminating the Device Limitation would comply with factors the Register uses to create a class. The Register's 2015 Recommendation explains that the determination of an appropriate class takes guidance both from Section 1201's language and legislative history. Under Section 1201, an exemption as part of the triennial rulemaking must be based on a "particular class of works."[73] These "particular class[es] of works" are the categories of works identified in 17 U.S.C. § 102, which include software under the category of literary works.[74] Congress has noted that "the 'particular class of copyrighted works' [is intended to] be a narrow and focused subset of the broad categories of works… identified in the section 102 Copyright Act."[75] But the Librarian "should not draw the boundaries of 'particular classes' too narrowly."[76]

Therefore, finding an appropriate class size requires that the Librarian draw classes where the prohibition on circumvention would affect the devices or things within that class in similar ways. Section 1201's legislative history provides two illustrative examples of overbroad and overly-narrow classes:

[71] 2015 Register's Recommendations at 317. Likewise, with regard to databases, the 2015 Register noted that "proponents presented no evidence in the course of the proceeding that demonstrated a need to access databases for purposes of security research. Accordingly, the discussion below excludes databases from consideration." 2015 Register's Recommendations at 253-54.

[72] CDT Initial Comments at 1, 3; USACM Comments; Green Comments at 1-2; *see* discussion *supra*, Section I.

[73] 17 U.S.C. § 1201(a)(1)(B).

[74] 17 U.S.C. § 102.

[75] H.R. Rep No. 105-551, Pt. 2, at 27

[76] Staff of H. Comm. on the Judiciary, 105th Cong., Section-by-Section Analysis of H.R. 2281 as Passed by the United States House of Representatives on August 4, 1998, at 7 (Comm. Print 1998).

1. A class that combined "prose creations such as journals, periodicals or books" and software would be overbroad because it is unlikely the prohibition on circumvention would affect both of them the same way;
2. On the other hand, subdividing classes such as motion pictures and television programs into particular genres would be overly narrow because the prohibition on circumvention will likely affect them the same way.[77]

The Register has also recognized that a "class of works" may be refined not just by the medium or the access controls, but also by "the particular type of use and/or user to which the exemption will apply."[78]

The differences between categories of functional devices in which software is embedded are much more similar to those between genres of television than to the differences between prose and software. Indeed, much like westerns or action shows share similarities in how they are broadcast and how the DMCA may affect criticism or educational studies on these shows, "genres of software" are part of a common platform of device software that shares similar vulnerabilities that security researchers seek to assess and suggest solutions to.

In this case, the prohibition on circumvention similarly affects security research on all types of software-enabled devices and systems. As multiple commenters have discussed, software now crosses over into a wide variety of different infrastructures and physical spaces.[79] Confining security research to some devices that have security vulnerabilities, but not others would overly cabin this class in contravention of Congressional intent.

### C. Allowing research on devices outside the Device Limitation will not endanger the public or create safety risks that are not already addressed by other laws.

Finally, some commenters argued that eliminating the Device Limitation would endanger the public. BSA argues that modifying the exemption may create "unique public safety risks and regulatory compliance considerations that would arise if the Device Limitation were eliminated."[80] The National Association of Secretaries of State, the Secretary of State of North Dakota, and ESP argue that, with regard to voting systems,

[77] *Id.*

[78] 2006 United States Copyright Office, Section 1201 Rulemaking: Third Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendations of the Register of Copyrights at 10, 19 (November 2006) ("2006 Register's Recommendations") (determining that "it can be appropriate to refine a class by reference to the use or user in order to remedy the adverse effect of the prohibition and to limit the adverse consequences of an exemption.").

[79] CDT Initial Comments at 1, 3; FSF at 2, USACM Comments.

[80] BSA Comments at 5.

expanding the Device Limitation would impact the critical infrastructure of the nation and expose significant national security risks.[81]

Eliminating the Device Limitation would not create any new or unique safety or security risks to critical infrastructure or otherwise. To the extent security flaws currently exist in non-exempt software, they will continue to persist—and be less likely to be fixed—if security researchers are unable to examine them. Security researchers perform their work specifically to assess potential security risks and assist in mitigating them necessary when.

While the continued inclusion of the Device Limitation will undoubtedly dissuade good-faith researchers from doing their work, it carries no corresponding upside for the security of currently non-exempt software. To the extent that malicious actors wish to discover and exploit vulnerabilities for nefarious purposes, there is no evidence on the record demonstrating that Section 1201 plays a meaningful role in deterring that behavior. This should be no surprise; copyright is not intended to serve as a tool for securing critical infrastructure, and the Constitution grants Congress the power to promulgate copyright law "[t]o promote the Progress of Science and the useful Arts," not national security.[82]

Moreover, a variety of already existing laws address these concerns more effectively than can copyright. For example, federal law already prohibits whoever intimidates, threatens, coerces, or attempts to intimidate, threaten, or coerce, any other person for the purpose of interfering with the right of such other person to vote or to vote as he may choose, or of causing such other person to vote for, or not to vote for," federal elected officials.[83]

Some commenters nevertheless contend that security researchers do not play an important role in addressing security risks and vulnerabilities. Essentially, the Secretary of State of North Dakota, NASS, and ESP argue that rigorous standardized processes, the Department of Homeland Security (DHS), and the U.S. Election Assistance Commission

[81] Comments of National Association of Secretaries of State (Feb. 13, 2018), https://www.regulations.gov/document?D=COLC-2017-0007-0136 ("NASS Comments"); Comments of the North Dakota Secretary of State (Feb. 13, 2018), https://www.regulations.gov/document?D=COLC-2017-0007-0137 ("North Dakota Comments"); ESP Comments at 4.

[82] *See* U.S. Const. art. I, § 8, cl. 8.

[83] 18 U.S.C. § 594 ("whoever intimidates, threatens, coerces, or attempts to intimidate, threaten, or coerce, any other person for the purpose of interfering with the right of such other person to vote or to vote as he may choose, or of causing such other person to vote for, or not to vote for, any candidate for the office of President, Vice President, Presidential elector, Member of the Senate, Member of the House of Representatives, Delegate from the District of Columbia, or Resident Commissioner, at any election held solely or in part for the purpose of electing such candidate, shall be fined or imprisoned not more than one year, or both."); *see also* discussion *infra*, Section III.

(EAC) already provide ample testing of election software security and so additional research is unnecessary.[84]

This stance contradicts opponents' broader claims. It cannot be the case that election software is so extraordinarily safe that independent security research is superfluous and simultaneously that permitting security researchers to analyze election software risks uncovering vulnerabilities so serious that their exposure could undermine national security.

The reality is that vulnerabilities in software, including election software, are still present and are under-researched because of the chilling effects of Section 1201.[85] Even ESP acknowledge that research performed on election software during an exercise at DEFCON exposed vulnerabilities.[86] Therefore, because all types of computer programs contain vulnerabilities, because there is no evidence that security researchers or anyone else have abused or are likely to abuse this exemption for nefarious purposes, and because there is substantial public benefit to finding and fixing vulnerabilities, the Register should recommend eliminating the Device Limitation.

## II. The record supports removing the Controlled Environment Limitation.

The Controlled Environment Limitation requires that circumvention is carried out, "in a controlled environment designed to avoid any harm to individuals or the public…"[87] The record supports the conclusion that this Limitation is ambiguous because the Limitation does not define the meaning of "controlled environment."[88] The record also shows that this limitation limits important testing in real-life environments that is necessary to ensure the secure day-to-day operation of computer systems.[89]

Prof. Felten and Prof. Halderman note, and CDT affirms, that the Register has not given any concrete guidance on what is considered a "controlled environment."[90] Our comments explain the significant and persistent chilling effect that results from security researchers not knowing if their good-faith effort to adhere to the Controlled Environment Limitation will hold up under actual or threatened litigation.[91] This ambiguity and its chilling effects have been demonstrated in the record, and the Office has not explicitly opined that this Limitation does not require limiting research to a lab-like setting. The proponents have not agreed that all uncontrolled testing is inappropriate, and in fact argue that real-life testing is in many cases necessary for effective research. Finally, security researchers follow strict norms and customs to prevent and mitigate any harm that may result from their testing.

[84] ESP Comments at 1, 11-12, 23; North Dakota Comments; NASS Comments.

[85] Felten Halderman Initial Comments at 4; CDT Initial Comments at 1.

[86] ESP Comments at 7-13.

[87] 37 C.F.R. § 201.40(b)(7).

[88] Felten Haldeman Initial Comments at 5.

[89] *Id.*

[90] CDT Initial Comments at 4.

[91] *Id.*

### A. The Controlled Environment Limitation is ambiguous and could create a burden to conduct research in a lab setting, chilling effective research.

Several opponents contend that the Controlled Environment Limitation is not ambiguous.[92] They argue the Limitation does not create a burden to conduct research in a lab like setting, but rather requires only reasonable research practices and mitigation of harm to the public.[93]

Specifically, BSA asserts that the Controlled Environment Limitation does not limit research to lab-like settings.[94] Instead, BSA contends that the Limitation merely requires researchers to mitigate harm to the public, and provides flexibility for researchers to adhere to norms protecting against harm.[95] The Joint Creators likewise argue that this Limitation simply mandates "reasonable research practices," and contend that Congress has provided guidance elsewhere as to what constitutes legitimate encryption research.[96] The Joint Creators also argue that the Controlled Environment Limitation has no objective deficiency in its regulatory clarity.[97] The Auto Alliance similarly argues that if there is any ambiguity, it can be resolved through legal challenges.[98]

Security researchers routinely and carefully design their testing to avoid public harm, and adhere to strict customs and norms.[99] These norms include responsible disclosure of vulnerabilities to the host entity, obtaining consent from system operators when needed to avoid user harm, and adhering to computer abuse laws.[100] In instances that involve human subjects, researchers comply with the Common Rule that protects any participants.[101]

This Limitation's ambiguity deters the kind of "good faith" research that would ultimately protect the public from dangerous vulnerabilities, and the chilling effect of this ambiguity is well-demonstrated in the record. Because the meaning of "controlled environment" is not defined, researchers remain uncertain about whether research in real-life settings would fall within the Limitation. Researchers need to test systems in real-life settings to understand how they work and to assess the variables that might come into play. Without

[92] Joint Creators Comments at 7; Comments of Alliance of Automobile Manufacturers, at 14 (Feb. 13, 2018), https://www.regulations.gov/document?D=COLC-2017-0007-0141 ("Auto Alliance Comments").

[93] Joint Creators Comments at 8; BSA Comments at 5.

[94] BSA Comments at 5.

[95] *Id.*

[96] Joint Creators at 8.

[97] *Id.* at 7.

[98] Auto Alliance Comments at 14.

[99] Felten Halderman Initial Comments at 31-32.

[100] *Id.* at 32 (citing 45 C.F.R. § 46).

[101] *Id.* at 32.

real-life testing, researchers will be left with an incomplete picture and potentially miss critical vulnerabilities and threats.

Eliminating the Controlled Environment Limitation would best resolve this adverse effect. As the Register noted, the uncertainty surrounding much of the language in the statutory exemption for security research creates a chilling effect for researchers.[102] However, it is not within the scope of the Office's authority under Section 1201—a proceeding concerned first, foremost, and only with the protection of copyrighted works—to set national policy on the contours for security research protocols. This task should be left to researchers and their various governing bodies.

Therefore, the best way to reduce uncertainty without unnecessarily constraining the development of research norms is to remove the limitation altogether. Alternatively, if the Office concurs with the notion advanced by BSA that the threshold for a "controlled environment" requires only that "harm to individuals or the public can be mitigated,"[103] a clarification in the final Recommendation to that effect would help (though not eliminate) the chilling effect of the limitation.

### B. Previous commenters did not agree that testing in real-life environments should be universally prohibited.

A number of objectors claim that every proponent in the 2015 Rulemaking agreed that live testing should never be allowed because of its potential safety risks.[104] ESP argue that there was universal agreement against testing in "live" conditions, citing the Register's conclusion that "in the context of a general security research exemption, there appeared to be universal agreement among proponents that testing in "live" conditions—such as cars being driven on public roads—is wholly inappropriate."[105]

These arguments conflate "live" testing with testing in real-life environments carefully designed to avoid harm. Good-faith security research would not be conducted on voting systems during a live election or on a vehicle on a public road. Strong ethical standards and customs—as well as other laws—preclude researchers' engagement in the kind of reckless research the opponents warn against.[106] Researchers draw a clear line between potentially harmful public testing and instances when there is a need to research in an uncontrolled environment.

The real issue researchers are concerned with is that this Limitation precludes all research conducted outside of a "controlled environment," even where safety is

[102] 2015 Register's Recommendation at 316.

[103] BSA at 5.

[104] ESP Comments at 13; Auto Alliance Comments at 13, Joint Creators Comments at 8.

[105] ESP Comments at 13 (*quoting* 2015 Recommendation at 318); Auto Alliance Comments at 13 (referencing the agreement that live testing is inappropriate and arguing that this is a common sense and necessary requirement as applied to motor vehicles).

[106] Felten Halderman Initial Comments at 31-32.

meaningfully accounted for.[107] Norms and regulations already prevent researchers from conducting the reckless testing examples the opponents use to generate an unfounded fear of what eliminating this Limitation would mean.[108] Testing in real-life environments is critical to finding vulnerabilities. Through self-regulation, peer review, and academic standards, researchers can mitigate any risks to themselves or the public.[109] Researchers must physically interact with devices in the field to find new vulnerabilities and new classes of vulnerable systems.[110] Many systems and whole classes of technology can only be thoroughly tested in the field, and limiting this research leaves the public exposed to serious and unknown cybersecurity threats.[111]

### C. Extending research to real-world environments does not expose researchers or the public to danger.

Several opponents speculate that opening up research to real world environments could place the researcher and public in danger.[112] More specifically, the National Association of Secretaries of State is concerned that these revisions may lead to "unfettered election hacking," pose significant challenges to officials, and undermine public confidence in the election system.[113] The Joint Creators assert that security researchers in support of this exemption admit that research in live setting is dangerous.[114] ESP argue that the Controlled Environment Limitation is critical to protect national election security, democratic principles, state laws, and public safety.[115] The Auto Alliance argues that the proponents have not cited any examples of this limitation having an adverse effect on security research for automobiles, and its removal could lead to heightened risks of property damage, injury, and death.[116]

While we are mindful of these concerns, public safety is *not* the province of copyright law or the Copyright Office.[117] Rather, Section 1201 is intended to protect copyrighted works against infringing activities. Opponents have not established in the record even a vague idea of how removing the Controlled Environment Limitation would lead to infringement of

[107] *Id.* at 21-23.

[108] *Id.*

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] The opposition commenters claim this Limitation is necessary to prevent researchers from circumvention of everything from commercial airplanes in flight to critical infrastructure like election systems on Election Day. NASS Comments; Joint Creators Comments at 8; ESP Comments at 13-14; Auto Alliance Comments at 13-14.

[113] NASS Comments.

[114] Joint Creators Comments at 8.

[115] ESP Comments at 13-14.

[116] Auto Alliance Comments at 13-14.

[117] Felten Halderman Initial Comments at 30.

copyrighted works. Indeed, their arguments point to supposed dangers stemming from lack of consent or cooperation from *system owners and operators* rather than *copyright holders*. This limitation adversely affects plainly non-infringing uses,[118] and opponents have not demonstrated or even contended that removing this Limitation will result in infringement.[119]

Even if the Copyright Office chooses to consider non-copyright concerns, the kind of research conducted by good-faith security researchers does not risk human injury or harm.[120] Strict norms and customs limit this research, and research that involves human subjects is properly regulated by the Common Rule.[121] Certain critical infrastructure can only be researched in the field,[122] and without this flexibility many vital systems that protect national security will go untested because of the Controlled Environment Limitation.[123]

Research has been and can be conducted by good-faith researchers in real-life environments in ways that avoid any danger to the public. As we explained in our initial comments, researchers conduct real-life security testing on systems with the consent of the system administrator while also adhering to other applicable laws.[124] For instance, a commercial jet was lawfully hacked by the Department of Homeland Security in 2016 in an uncontrolled setting in a way that ensured the safety of the public.[125] Likewise, researchers are conducting Internet-wide scanning involving small numbers of harmless connections to publicly accessible computers to analyze trends and the security of the Internet itself.[126] Another example is testing the security of building automation systems such as heating and air conditioning in real-world settings and in real-time.[127]

## III. The record supports removing the Other Laws Limitation.

The current exemption for security research requires that circumvention be performed only on a "lawfully acquired" device or machine and not violate "any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986, as amended and

[118] *Id.* at 9-17.

[119] *Id.* at 9-17.

[120] *Id.* at 38.

[121] *Id.* at 38-39.

[122] *Id.* at 33. This includes facilities and infrastructure in the chemical, commercial, manufacturing, communications, energy, water, food, health, and transportation sectors. *Critical Infrastructure Sectors*, Homeland Security, https://www.dhs.gov/critical-infrastructure-sectors (last visited Mar. 13, 2018).

[123] *Id.* at 33, 38-39. We also note that infrastructure research depends on an expansion of the device limitation. *See* discussion *supra*, Section I.

[124] Felten Halderman Initial Comments at 21-22; CDT Initial Comments at 2-4.

[125] Felten Halderman Initial Comments at 22.

[126] *Id.* at 22.

[127] *Id.* at 22-23.

codified in Title 18, United States Code."[128] The record supports the conclusion that the phrase "lawfully acquired" is ambiguous because contractual restrictions cloud the concept of ownership. Likewise, the "other laws" provision creates uncertainty because it requires researchers to predict how a court might interpret a notoriously unclear law. Contrary to opposing commenters' assertions, removing these limitations will not lead to unlawful circumventions because triennial exemptions do not preclude liability under any other laws, which are already sufficiently deterrent.

### A. Opposing commenters illustrate the ambiguity surrounding "lawful acquisition."

In the initial comment round, several proponents noted that the "lawfully acquired" portion of the Other Laws Limitation in the existing security research exemption inhibits beneficial research because of the uncertainty it creates.[129] Specifically, Prof. Felten and Prof. Halderman noted that licensing agreements restricting the use or resale of software or devices raise questions about researchers' ability to lawfully acquire or merely gain access to copies of software for research purposes.[130]

Opposing commenters helpfully illustrate how these agreements obstruct research, claiming that software distribution is sufficiently restricted by license terms to preclude researchers' ability to obtain a copy. For instance, ESP put forward an argument nearly identical to the hypothetical situation described in the Felten and Halderman initial comment.[131] ESP take a particularly defensive stance, stating that even the election officials to whom they license software cannot "own" those copies and therefore cannot rely on Section 117 to "immunize" them from infringement under Section 106.[132]

Other opponents raise this issue as well, attempting to circumscribe the scope of software ownership by consumers through the use of licensing agreements structured to align with favorable judicial precedent.[133] In light of opposing commenters' vocal endorsements of using licensing agreements to expand the scope of their control over software copies beyond the bounds of copyright and other laws, and the corresponding

[128] 37 C.F.R. 201.40(b)(7)(i).

[129] Felten Halderman Initial Comments at 23; CDT Initial Comments at 4; Rapid7 (Dec. 19, 2017), https://www.regulations.gov/document?D=COLC-2017-0007-0095 ("Rapid7 Comments").

[130] Felten Halderman Initial Comments at 23.

[131] ESP Comments at 17; Felten Halderman Initial Comments at 23.

[132] ESP Comments at 18.

[133] Joint Creators Comments at 9 n.6 (citing Vernor v. Autodesk, Inc., 621 F.3d 1102, 1110-11 (9th Cir. 2010)).

reduction in consumers' usage and possessory rights, researchers understandably view "legal acquisition" as a source of uncertainty with regard to copies of software.[134]

This uncertainty is greater in instances where the software does not reside in a physical object purchased by the researcher, such as building HVAC systems, or where software is provided as a service. In those cases, it may be difficult or impossible for researchers to "acquire" the software in the context of ownership, and the current ambiguity may preclude researchers from pursuing these projects for fear of incurring legal liability. Moreover, the "lawfully acquired" limitation fails to account for other common unknown variables in the course of security research. For instance, to the extent that the limitation allows for acquisition by parties other than the researchers, the researchers may not have the information necessary to determine the legality of the third party's acquisition. Finally, for some kinds of computer programs, such as malware, a legitimate market may not exist, making it impossible to legally obtain a copy. While this research is no less important to preserve the safety of the public, study of potentially malicious software may be impeded by the current language of the exemption, which does not account for the realities of this particular marketplace.

### B. Removing the "lawful acquisition" limitation will neither allow nor incentivize illegal research activity.

Opponents cite an analogy from the DMCA's legislative history as evidence of congressional intent that an exemption for liability under Section 1201 should be limited by the Other Laws Limitations.[135] This analogy posits that security testing is fine for "door locks" purchased and installed on the researcher's home, but not permitted for locks on doors belonging to others.[136]

However, the analogy assumes ownership as the only model and does not account for the fact that software users, whether owners or licensees, have the same interests in security regardless of their contractually defined possessory interests. Even though purchasers of software may not "own" the software, at least for the purposes of the license provisions, they should still be able to test its security, especially when software collects, creates, or stores information about the user. However, rather than acknowledging the complexity of current possessory interest models, opposing commenters use the simplicity of the original analogy as evidence of the clarity of the "lawfully acquired" limitation, while at the same time arguing against the kind of ownership it assumes.[137]

[134] ESP Comments at 17. ("[ESP] believe that independent security researchers who are not working collaboratively with the provider of the applicable product could not acquire a copy of election software without violating the applicable License.")

[135] Joint Creators Comments at 9; BSA Comments at 6 (citing H.R. Rep. No. 105-796 at 67 (1998)).

[136] H.R. Rep. No. 105-796 at 67 (1998)).

[137] Joint Creators Comments at 9 n.6.

In the 1201 Policy Study, the Register recommended adding greater flexibility to the authorization requirement in 1201(j).[138] Replacing the authorization condition with the "lawfully acquired" requirement was an improvement to the scope of the triennial exemption. However, for the reasons discussed above, the "lawfully acquired" limitation remains a source of uncertainty for good-faith researchers. If the Office declines to recommend the removal of this language, we respectfully suggest that researchers would benefit from clarification regarding the interplay between licensing agreements and legal acquisition, acquisition by third parties, as well as how the words "legally acquired" apply in instances where physical possession of a computer program is not possible.

### C. The inferred intent of Congress should not prevent the Register from recommending changes to elements of the language used by 1201(j).

The Register concluded that using the "other laws" provision from 1201(j) preserved the intent of Congress to enable only lawful research.[139] However, with regard to the level of deference opponents and the Office give to Congress's inclusion of the "other applicable laws" limitation in 1201(j),[140] it is our position that, like many other aspects of 1201(j), this provision may not have helped Congress fully achieve its aim to enable good-faith security research.[141] Its inclusion in the exemption, therefore, should not be considered any more necessary than the authorization requirement or the non-exclusive factor list,[142] which the Office has previously recommended against.[143]

As the Register correctly observed, "other laws still apply even if the activity is permitted under Section 1201."[144] It is clear why theft or trespassing should trigger liability for theft or trespassing. Likewise, a circumvention amounting to a violation of the CFAA should be penalized under that statute, but it is unclear why researchers should also be penalized under Section 1201 for an activity otherwise permitted by an exemption from Section 1201. By removing this limitation from the exemption, the Office could reduce

[138] Section 1201 of Title 17: A Report of the Register of Copyrights, at 77 (June 2017), https://www.copyright.gov/policy/1201/section-1201-full-report.pdf ("1201 Policy Study"); *see also* 17 U.S.C. § 1201(j).
[139]2015 recommendations at 318.
[140] *See e.g.*, Joint Creators at 3.
[141] Felten Halderman Initial Comments at 24-25 ("Indeed, it would not have been necessary for Congress to delegate the authority to create new exemptions if the permanent exemptions were sufficient to protect from future harm. Rather, Congress entrusted the Office to create exemptions that protect noninfringing use from unanticipated future harm.")
[142] § 1201(j)(1), (j)(3).
[143] 1201 Policy Study at 80 (June 2017).
[144] *Id.*

liability risk and uncertainty for researchers within the ambit of Section 1201 without diluting pre-existing statutory protections against piracy.

### D. Opposing commenters agree that "other laws" are a source of uncertainty.

Even if Congress intended to add DMCA liability to liability for circumventions in violation of other laws, it could not have foreseen the interpretive miasma that has developed around several key terms in Section 1030 of the CFAA, including "accessing" and "exceeds authorized access."[145] Because of the difficulty of determining whether certain acts would trigger CFAA liability, and therefore also trigger DMCA liability, researchers must avoid research projects that hold any potential to implicate the CFAA. We agree with commenters who note that avoidance of CFAA liability is more likely to inhibit research than a risk of DMCA liability.[146] We also agree that the "other laws" themselves are a greater source of uncertainty than the "other laws" limitation.[147] Unfortunately, the "other laws" limitation incorporates the uncertainty of those laws into the exemption. The wording of the limitation is relatively clear, but a court's interpretation of the laws it references is not. Therefore, the additional liability imposed by the "other laws" limitation is redundant and unnecessary, adding only an extra source of liability and an extra source of uncertainty for researchers attempting to work within the bounds of the DMCA exemption.

### E. The deterrent effect of the CFAA renders additional DMCA liability unnecessary and redundant.

Given the stiff penalties potentially imposed under the CFAA, exempting researchers from liability under the DMCA is unlikely to lead to the rampant lawless behavior suggested by opponents.[148] Nor would removal of the "other laws" limitation waive the applicability of those laws. Therefore, eliminating this limitation would improve the exemption by reducing uncertainty but would not incentivize illegal acts or increase public safety risks. If the Office declines to remove this limitation, we respectfully suggest that converting the limitation to a reminder that the exemption "does not obviate the need for compliance with other laws," in

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

[146] Auto Alliance Comments at 13.

[147] Auto Alliance Comments at 12.

[148] *Id.* at 11; SIIA Comments at 4-5; 18 U.S.C. § 1030(c).

accordance with the NTIA's recommendations, would preserve Congress's intent to encourage only lawful acts of security research.[149]

## IV. The record supports removing the Access and Use Limitations.

The current exemption for security research limits circumvention to instances undertaken "solely for the purpose of good-faith security research," which means accessing a computer program "solely for purposes of good-faith testing, investigation, and/or correction" of flaws or vulnerabilities.[150] The exemption 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."[151]

Respectively, these are the Access and Use Limitations. The record supports the conclusion that the Access Limitation chills legitimate security research because a strict reading of the word "solely" excludes beneficial activities associated with security research, such as teaching and scholarship. Likewise, the record supports the conclusion that the Use Limitation chills legitimate research because it creates uncertainty as to researchers' obligations with regard to the use and maintenance of the information derived from research. Contrary to opponents' assertions, removing these limitations would not disrupt well established norms, such as coordinated vulnerability disclosure, nor would researchers be encouraged to perform or use research for unlawful purposes. Finally, proponents need not prove that all possible uses of works protected by TPMs will be non-infringing, only that their ability to make non-infringing use of works is adversely affected.

### A. Removing the Access and Use Limitations will not disrupt existing disclosure practices.

Opponents claim that removing the Access and Use Limitations would spur researchers to disregard common practices, such as reporting vulnerabilities to the party responsible for issuing a patch whenever possible.[152] Instead, opponents contend that researchers would default to immediate public disclosure, thereby upsetting established relationships and thwarting cooperation between independent researchers and makers of software and devices.[153]

[149] Recommendations of the National Telecommunications and Information Administration to the Register of Copyrights, at 58, 72 (Sept. 8, 2015), http://copyright.gov/1201/2015/2015_NTIA_Letter.pdf.
[150] 37 C.F.R. § 201.40(b)(7)(i), (ii).
[151] 37 C.F.R. § 201.40(b)(7)(ii).
[152] Auto Alliance Comments at 3, 11, 15; ESP Comments at 20.
[153] *Id.* Auto Alliance and ESP also appear to contend that restricting disclosure by researchers does not raise First Amendment concerns. Auto Alliance Comments at 12, 14; ESP Comments at 24. Neither opponent grapples substantively with our explanation of why

To the contrary, researchers do not seek a more adversarial relationship with vendors, nor would removing the limitations create such an incentive. Rather, those relationships and the disclosure norms that have grown out of them are shaped by many factors unrelated to the language of the security research exemption.

As commenters observe, collaboration between independent researchers and vendors has significantly increased.[154] However, this increased level of collaboration owes nothing to the limitations within the exception and everything to the improved legal status of good-faith security research as well as vendors' acceptance of the value of independent research.[155] Instead of a defensive attitude toward researchers, more vendors have adopted positive approaches to receiving and responding to vulnerability notifications. This has made it easier for researchers to work with vendors and has promoted coordinated disclosure as the preferred option.

Removing the limitations will make independent research legally possible on more software-dependent devices and systems, which will encourage even more cooperation and coordination between researchers and software companies, resulting in more secure products. Similarly, even without the "Use" or "Access" Limitations in the 1201 exemption, researchers have little incentive to bypass coordinated disclosure unless vendors are unresponsive or adversarial.[156] Therefore, their removal from the exemption would not encourage irresponsible disclosure practices, but would reduce the uncertainty researchers face when trying to determine whether their actions will be seen as having been "solely" for the purpose of good-faith research and "primarily" used to promote safety and security.

### B. Removing the Access and Use Limitations will not promote illegal activity or increase public safety risks.

Opposing commenters claim that eliminating the Access and Use Limitations would "allow" researchers to use research performed under the exemption as a pretense for any number of ulterior motives.[157]

limitations on disclosure raise significant constitutional concerns; we incorporate our discussion from our initial comments by reference here. Felten Halderman Initial Comments at 6, 24, 29, 33; CDT Initial Comments at 5.

[154] Auto Alliance Comments at 15.

[155] National Telecommunications and Information Administration, Vulnerability Disclosure Attitudes and Actions: A Report from the NTIA Awareness and Adoption Group, at 8 n.7, 9-10, 11 (2016), https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf.

[156] *Id.* at 5.

[157] Auto Alliance Comments at 5; Joint Creators Comments at 10-11; ESP Comments at 15-16; NASS Comments; SIIA Comments at 2.

The Section 1201 exemption process does not and cannot preclude liability under any other law or legal theory. Moreover, the kinds of motives, acts, and resulting harms put forward by opposing commenters would eclipse any interpretation of "good faith" and render the proposed exemption inapplicable.[158] Third, to the extent that purposes beyond good-faith research and uses beyond promoting safety and security are lawful and non-infringing, they should be permitted because enabling non-infringing use is the purpose of 1201 exemptions.[159]

### C. Opponents illustrate the uncertainty of the Use Limitation.

Commenters claim that the Use Limitation is unambiguous, but their collective comments illustrate some of the many possible interpretations of the Use Limitation. ESP and Auto Alliance imply that the limitation requires coordinated disclosure, or at least an attempt to contact the vendor, while also acknowledging, as the Register has, that contacting vendors or developers, even when they can be identified, is not always possible.[160] Auto Alliance further claims that the actions of third parties cannot trigger liability for researchers, but also states that "premature" disclosure could facilitate violations of applicable laws by informing bad actors of a vulnerability.[161]

Likewise, the Joint Creators state that the "exemption simply holds researchers responsible for handling their own results with care to prevent others from misusing them to the extent feasible."[162] Yet this still requires researchers to predict how third parties will use the results and whether those uses will be infringing.

For risk-averse researchers, this requires assuming the worst: that third parties will use research to infringe copyrights. Even under a less extreme risk model, there is at least some possibility that research will "facilitate" infringement. How are researchers to determine whether their risk assessment and resulting decisions about the use and maintenance of their research will match up with a retrospective view of events? This calculus becomes more complex for projects involving more than one researcher. Opponents offer little guidance here.

To the extent opposing commenters offer guidance, their interpretations of the types of uses allowed by the existing Use Limitation vary. Some commenters propose that teaching peer review would be acceptable under the "use" limitation.[163] Others imply that the Use

[158] ESP Comments at 20.

[159] 17 U.S.C. § 1201(b), (c); 1201 Policy Study at i-ii.

[160] ESP at 15 (labeling the 2nd prong of the Use Limitation as the "coordinated disclosure limitation"); Auto Alliance Comments at 3, 11, 15; Joint Creators Comments at 11; 2015 Register's Recommendations at 309.

[161] Auto Alliance Comments at 16.

[162] Joint Creators Comments at 11.

[163] ESP Comments at 15.

Limitation prevents making research "available."[164] ESP oppose researchers' ability to alert the public to vulnerabilities in voting machines "because voters do not get a choice of what technology to use at their local polling place," implying that disclosure in this circumstance would not comport with the existing "use" limitation.[165] The inconsistency with regard to what the Use Limitation permits or prohibits illustrates the limitation's ambiguity.

### D. Proponents need not show that all possible uses are non-infringing.

Opposing commenters claim that proponents have not met the required burden of proof under a variety of theories. Some propose that research is not being inhibited by access controls and Section 1201, offering the publication of research, coordinated disclosure programs, and industry growth as evidence that neither research nor publication are chilled by the Use Limitation.[166] This is incomplete logic. Publication of some research does not mean that other beneficial research projects and discussions are not inhibited by the limitation. Instead, opponents would have proponents prove the absence of research or the non-existence of published research. But 1201(c) does not require proof of a negative, it merely requires the Librarian to determine whether the prohibition on circumvention is or is likely to adversely affect noninfringing uses of copyrighted works protected by access controls.[167]

Others imply that proponents must prove that any uses beyond good-faith research will be non-infringing.[168] This is also more than the statute demands. Here, researchers wish to perform good-faith security research on computer programs, a use which the Register has previously determined to be noninfringing.[169] They are adversely affected by the prohibition because the uncertainty created by the exemption's Use Limitations chills their ability to make full use of the exemption. Therefore, the record supports removal of this limitation.

[164] Comments of DVD CCA & AACS LA, at 3 (Feb. 13, 2018), https://www.regulations.gov/document?D=COLC-2017-0007-0150 ("DVD CCA & AACS LA Comments") (also proposing that removing the Use Limitation could lead to research advancing circumvention techniques).

[165] ESP Comments at 16 n. 64.

[166] Auto Alliance Comments at 5-8; App Association Comments at 3; SIIA Comments at 4.

[167] 17 U.S.C. § 1201(c).

[168] Auto Alliance Comments at 5 ("In addition, removal of the Use Limitation or the Good Faith Limitation raises questions regarding whether the copy or adaptation of a computer program enabled by circumvention will be used in "no other manner" than in conjunction with a machine, as required by 17 USC § 117(a)(1) in order for the activity to be non-infringing. Therefore, any expansion of the existing exemption must be carefully examined to determine whether it enables uses likely to be noninfringing.")

[169] 2015 Register's Recommendation at 300 ("The Register finds that the overall record supports proponents' claim that accessing and reproducing computer programs for purposes of facilitating good-faith security research and identification of defects are likely to be fair uses of the programs under section 107.")

*　　*　　*

For the foregoing reasons, the Register should recommend the removal of the Device, Controlled Environment, Other Laws, Access, and Use Limitations.