This is a Word document that allows users to type into the spaces below. The comment may be single-spaced, but should be in at least 12-point type. The italicized instructions on this template may be deleted.

UNITED STATES COPYRIGHT OFFICE

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

ITEM A. COMMENTER INFORMATION

The commenter is the Center for Democracy & Technology (CDT), a non-profit advocacy organization dedicated to the advancement of democratic values in the digital age. The organization is located at 1401 K St. NW, Suite 200, Washington, DC 20005. The contact for the organization is Ferras Vinh, who can be reached via email at fvinh@cdt.org or by phone at (202) 407-8827.

ITEM B. PROPOSED CLASS ADDRESSED

Proposed Class 10: Computer Programs – Security Research

ITEM C. OVERVIEW

The expanded exemption sought is for software security research, which provides essential protections for active research and testing efforts into evolving cybersecurity risks. The Copyright Office has acknowledged the value of this research, as evidenced by the decision to renew the pre-existing exemption.[1] However, the exemption contains restrictions on research methods and eligible devices, which limits and chills critical research into vulnerabilities with the threat of litigation.

As we have noted in previous exemptions, software and related access controls are increasingly embedded in a wide range of systems. The Register recognized this by granting an exemption for software security research during the last triennial period that included consumer devices, medical devices, and motor vehicles.[2] But the exemption did not include other types of devices that increasingly include software and will also feature security flaws and vulnerabilities, like infrastructure and industrial equipment. Due to the widespread integration of software in tangible 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.

In light of the rapid proliferation of products and systems subject to software-based security flaws and vulnerabilities, an exemption needs to cover more than just a single product or class of

[1] Exemptions to Permit Circumvention of Access Controls on Copyrighted Works, 82 Fed. Reg. 49550, 49555 (Oct. 26, 2017) (to be codified at 37 C.F.R. pt. 201).
[2] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 37 C.F.R. pt. 201.40(7).

product. Product-by-product exemptions (e.g., software contained in smart thermostats) would make little sense in a world where harmful flaws may exist in any of a wide variety of products or systems. If researchers are forced to wait for the next triennial review process each time they discover that software on an additional type of specific product carries significant security vulnerabilities, the damage will already be done.

For these reasons, the Copyright Office should grant the petitions for a broader exemption covering security research under Proposed Class 10.

ITEM D. TECHNOLOGICAL PROTECTION MEASURE(S) AND METHOD(S) OF CIRCUMVENTION

The access control measures relevant to this exemption will likely include challenge-response mechanisms such as access codes, passwords, keys, or digital signatures; encryption; and software features designed to prevent tampering with or changing the software, such as code obfuscation and runtime checks. Security researchers must also must be able to reverse engineer malware to protect computers, systems, and their users.

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

As the Register noted in its recent study, Congress enacted section 1201(j) out of concern that "[s]ection 1201(a) could be construed to inhibit legitimate forms of security testing."[3] Accordingly, the need to shield and encourage this research has gained consensus support, as illustrated by the recommendation of the Office to renew the pre-existing exemption. Without this exemption, the anti-circumvention provisions of the DMCA serve as a significant barrier to research on software flaws and vulnerabilities.[4]

The exemption provides a protective legal umbrella, allowing researchers to ensure the safety of devices and machines used on an everyday basis without the chilling effect of potential litigation. By renewing and expanding the exemption, the Register can encourage research that will help address dangerous gaps in public safety. In a recent report, "The Importance of Security Research," CDT identified several notable examples of such research, including the following:[5]

- **Automotive Security Research:** In 2015, security researchers discovered flaws in Chrysler, Dodge, and Jeep vehicles that use the UConnect system.[6] Independent security researchers Charlie Miller and Chris Valasek discovered vulnerabilities in the system that would allow a malicious actor to turn off the engine, unlock the car, and control the

[3] U.S. Copyright Office, Section 1201 of Title 17 at 19 (June 2017).
[4] Petition of Profs. Bellovin, Blaze, Felten, Halderman, and Heninger at 3 (2015).
[5] With the exception of the WhiteScope security research, all of the following examples are described in the aforementioned report.
[6] Joseph Lorenzo Hall, Apratim Vidyarthi, and Benjamin C. Dean, Center for Democracy & Technology, The Importance of Security Research 3 (2017).

steering wheel, brakes, transmission, and acceleration.[7] The results were disclosed to the public, and Chrysler recalled more than 1.4 million vehicles.[8] Similar flaws were identified by academic security researchers in other investigations conducted in more controlled experimental conditions, but were not acted upon.[9]

- **Medical Devices:** Multiple studies from security researchers have highlighted vulnerabilities in implanted defibrillators and pacemakers that leave them susceptible to malicious software attacks, ransomware, or accidental malfunctions.[10] For instance, security researchers discovered a flaw that would allow malicious actors to hack a pacemaker and deliver a fatal shock to a patient.[11] Despite the fact that the issue was identified in April 2015, no patch for it has been released.[12] More recently, security researchers at WhiteScope were able to investigate and uncover more than 8,000 known vulnerabilities in pacemaker software, flagging issues that require immediate attention from manufacturers and potentially creating a safer product for consumers.[13]
- **Voting Systems:** In July 2017, security researchers were able to subvert every piece of voting equipment at the Voting Village at the DEFCON hacking conference within 24 hours. Notably, researchers were able to remotely control the AVS WinVote system, which was largely used in Virginia from 2004 through 2015. The attacker was able to manipulate both the ballot display and the electronic recording of votes in a completely automated fashion.
- **Consumer Devices:** In 2016, researchers at the University of Michigan created malware to target a home security/alarm system that provided access to the PIN; remote control of the blinds, lights, and other connected home functionalities; and the ability to turn on the fire alarm. Many security systems are vulnerable to these problems, as they are particularly susceptible to jamming and transmit unencrypted signals on wireless networks.

But while the current exemption has helped promote essential security research in this vein, the limitation on devices does not account for the software and access controls increasingly embedded in a wide range of other critical systems, including infrastructure and industrial equipment.[14] For example, researchers have sought to evaluate and ensure the security of encryption modules for financial transactions like ATM withdrawals, toll collection, and

[7] *Id.* at 3.
[8] *Id.* at 4.
[9] *Id.*
[10] *Id.* at 6.
[11] *Id.*
[12] *Id.*
[13] Billy Rios, Understanding Pacemaker Systems Cybersecurity, WhiteScope IO (May 23, 2017, 9:44 AM), http:// blog.whitescope.io/2017/05/understanding-pacemaker-systems.html.
[14] *See also* Rapid7 et al., Joint Comments to US Copyright Office Notice of Inquiry (Docket No. 2015-8), Library of Congress 1201 Study at 4-5, Oct. 27, 2016 (noting ambiguity in temporary exemption under Section 1201 regarding what software qualifies for the exemption).

infrastructure that communicates with computerized vehicles.[15] The current limitation does not account for the expanded use of TPMs in other systems, and constrains research that would make these devices safer and more secure.[16]

Moreover, the requirements that circumvention must be "solely" for the purpose of good-faith security research and that such search involves accessing a computer program "solely" for purposes of good-faith testing, investigation, or correction of a security flaw should be removed. Under these requirements, it is unclear whether academic research and open public discussion of vulnerabilities fall within the exemption, placing legal constraints on the study and prevention of critical flaws. These discussions among peers and experts can help researchers gain a greater understanding of the system or the technology beyond the vulnerability itself, as the learning process often spans beyond a singular goal or objective. But as a consequence of the current restrictions, researchers may be limited in their opportunities to build upon their initial discoveries through discussions with peers and the general public, foreclosing opportunities to expand their base of knowledge and identify future flaws in software.

Further, the condition that circumvention does not violate the Computer Fraud and Abuse Act of 1986 (CFAA) should be removed to reduce uncertainty and risk for researchers. Because section 1201(j) incorporates the CFAA, a court's adverse construction of "exceeding authorized access" under the CFAA would expose a researcher to liability under both the CFAA and section 1201.[17] Granting an exemption to strike this language would not shield researchers from liability under other laws—it would merely provide them with greater certainty, particularly given that the scope of CFAA has not been uniformly interpreted across judicial circuits.[18] To address this issue, the Register could also replace the language with a provision that states that the exemption "does not preclude liability under other applicable laws."[19]

The Office should also remove the restriction of security research to the setting of a "controlled environment designed to avoid any harm to individuals or the public" to reduce ambiguity for researchers. While the aims of the Office are understandable in this context, the Register did not provide any concrete guidance as to what constitutes a controlled environment. Subsequently, researchers are forced to develop their own set of norms without knowing that they will hold up in a court of law. Accordingly, many researchers may choose to forego or withhold research rather than face critical legal scrutiny and liability.

---

[15] Mitch Stoltz et al., Additional Comments of the Electronic Frontier Foundation in the Matter of Section 1201 Study at 7, October 27, 2016.
[16] Matthew Green, *Statement on DMCA lawsuit*, A Few Thoughts on Cryptographic Engineering (July 28, 2016), https://blog.cryptographyengineering.com/2016/07/28/statement-on-dmca-lawsuit/.
[17] Erik Stallman and Stan Adams, Comments of the Center for Democracy & Technology before the United States Copyright Office, Library of Congress Section 1201 Study at 11, March 3, 2016.
[18] *Id.* at n. 52.
[19] NTIA Recommendations at 58, 62.

Additionally, the restriction on the post-circumvention use of the "information derived from the activity" should be removed to protect the First Amendment rights of researchers and to shield researchers from liability for the actions of independent third parties. The limitation chills the discussion of vulnerabilities by requiring that the information be used "primarily" to promote the security or safety of devices or machines. Under this provision, researchers (1) must discern what proportion of discussion about a vulnerability constitutes "primarily" and (2) take responsibility for what another party does with the information. As a result, researchers may choose to forego or slow down research efforts by shutting down dialogue with potential partners and withdrawing from peer reviews and evaluations of the relevant work.

Finally, the limitation for security research to a "lawfully acquired device or machine" should be removed from the exemption. While we recognize the need to protect the *physical* property of individuals, copyright protections are intended to protect *intellectual* property rights. But with this language in place, an individual would incur the additional severe penalties of a copyright offense for what constitutes a criminal offense. With this in mind, the theft of physical property should remain outside the scope of copyright law and enforcement.

DOCUMENTARY EVIDENCE

As documentary evidence, we have attached the "The Importance of Security Research" report authored by Joseph Lorenzo Hall, Apratim Vidyarthi, and Benjamin C. Dean at CDT. The case studies in the report detail some of the more notable discoveries in security research in recent years and help illustrate the importance of an exemption to the DMCA.