**Comment Regarding a Proposed Exemption Under 17 U.S.C. Section 1201 for Software Security Research (Class 25)**

**February 6, 2015**

## 1. Commenter Information

Professor Candice Hoke, Cleveland State University*
Professor Douglas W. Jones, University of Iowa*
Professor Deirdre Mulligan, University of California, Berkeley*
Professor Vern Paxson, University of California, Berkeley*
Professor Pamela Samuelson, University of California, Berkeley*
Bruce Schneier
Erik Stallman, Center for Democracy & Technology (CDT)

* Affiliation for identification purposes only

Contact person: Erik Stallman, CDT, (202) 407-8817, estallman@cdt.org

## 2. Proposed Class Addressed

These comments address Proposed Class 25: Software – Security Research.

## 3. Overview

An exemption for software security research is essential to promote the active research and testing efforts necessary to keep pace with evolving cybersecurity risks.

Software and related access controls are increasingly embedded in a wide range of systems, from consumer goods to medical devices to infrastructure to industrial equipment. This trend carries tremendous opportunities, but it inevitably will bring a raft of new security flaws and vulnerabilities as well. 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. The emergence of the Internet of Things is one example of the spreading risk.[1]

In this rapidly evolving environment, active security research and testing are crucial. Without an exemption, however, the DMCA's anti-circumvention provisions will substantially chill such research, for the same reasons the Copyright Office cited in

[1] Federal Trade Commission, internet of things: Privacy and Security in a Connected World, Jan. 2015, http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

granting previous exemptions for CD and video game security testing: the scope of the security exception in 1201(j) is simply not clear[2] and that lack of clarity chills the kind of security research that needs to happen today.

Given the rapid proliferation in the kinds 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 product. Product-by-product exemptions – say, for security research regarding the software contained in Internet-connected thermostats – would make little sense in a world where harmful flaws may exist in any of a wide variety of products or systems. Security researchers need appropriate legal latitude to engage in good faith security research. 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. In a world moving at Internet speed, security researchers cannot help protect the public if each new research effort has to be put on hold until the next triennial permission cycle.

For these reasons, the Copyright Office should grant the petitions for an exemption covering good-faith security research. Without such an exemption, security risks will lie unaddressed and the public will be substantially less safe.

## 4. Technological Protection Measures and Methods of Circumvention

As set forth in the petitions for a software security research exemption, the access control technologies 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 also must be able to reverse engineer malware to protect computers, systems, and their users.

## 5. Asserted Noninfringing Uses

In the 2010 recommendation for a video game security research exemption, the Register concluded that:

> the factors set forth in 17 U.S.C. 107 tend to strongly support a finding that such good faith [security vulnerability] research constitutes fair use. The socially productive purpose of investigating computer security and informing the public do not involve use of the creative aspects of the work and are unlikely to have an adverse effect on the market for or value of the copyrighted work itself.[3]

---

[2] *See* 77 FR 68427, 68477 (Nov. 27, 2006).
[3] 75 Fed. Reg. 43833 (July 27, 2010).

The identical logic applies here. Good faith security research for the purpose of identifying potentially harmful security flaws and vulnerabilities constitutes a non-infringing use of the software subjected to such research and testing.

**6. Asserted Adverse Effects**

Without an appropriate exemption, the DMCA's anti-circumvention provisions create a significant barrier to research on software flaws and vulnerabilities. The computer security researchers listed above are all aware of instances in which they or their colleagues have refrained from conducting or disseminating security research due to legal fears stemming from the DMCA. The prominent security researchers who submitted the exemption petitions have stated that they have chosen not to perform or disseminate security research that could have benefitted public safety because of the legal risks.[4] A group of corporate computer security leaders representing nearly 50 companies have stated that the DMCA "hamper[s] both our ability to protect our businesses and the public from information security threats and to conduct critical security research."[5]

As the Register concluded in 2010, Congress recognized the importance of not discouraging computer security research: "Section 1201(j) is evidence of Congress's general concern to permit circumvention under appropriate circumstances for purposes of security testing."[6] But the existing security testing exemption in section 1201(j) is insufficient to ensure that the anti-circumvention provisions will not chill research on systems security, for at least two reasons.

First, as the Register concluded in both 2010 and 2006, "it is unclear whether Section 1201(j) applies in cases where the person engaging in security testing is not seeking to gain access to, in the words of Section 1201(j), 'a computer, computer system, or computer network.'"[7] This same ambiguity is fully applicable to security testing of software associated with numerous devices and systems.

Second, Section 1201(j) requires that testing be done "with the authorization of the owner or operator of such computer, computer system, or computer network."[8] This creates additional ambiguity, as it seems to reflect an assumption that security testing will be performed by employees or agents of the entity deploying or using computer systems and associated software. In an Internet-connected environment, some security testing may need to be performed by independent security researchers. It is far from clear that all relevant parties would readily provide

---

[4] Petition of Profs. Bellovin, Blaze, Felten, Halderman, and Heninger at 3.
[5] See Coalition for Security Research, *Support DMCA and CFAA Reform to Protect Security Research,* https://www.c4sr.org.
[6] 75 Fed. Reg. 43833 (July 27, 2010).
[7] 75 Fed. Reg. 43833 (July 27, 2010).
[8] 17 U.S.C. 1201(j)(1).

authorization for research that could expose embarrassing flaws or vulnerabilities in their products.

Granting the petitions for a software security exemption would promote security research by providing greater clarity and certainty to researchers. Without such an exemption, the public will face reduced security and significantly elevated risk of harm from security flaws and vulnerabilities.