Before the

U.S. COPYRIGHT OFFICE, LIBRARY OF CONGRESS

Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. § 1201

Docket No. 2014-07

Response to Post-Hearing Questions for Class 25: Software-Security Research

Commenters

Laura Moy, New America's Open Technology Institute
Andy Sayler, Center for Democracy & Technology[1]
Erik Stallman, Center for Democracy & Technology

Contact: Erik Stallman, erik@cdt.org, (202) 407-8817

1. The Office should not attach a disclosure requirement to the proposed exemption.

Choosing whether and how to disclose a security vulnerability is a complex, situation-specific question that requires substantial discretion for the researcher and is not well-suited to inflexible standards or timelines.[2] Even opponents of the proposed Class 25 exemption acknowledge that "every vulnerability is different, and that the fix to every vulnerability may take a different amount of time."[3] Accordingly, and as in past recommendations related to cybersecurity, we request that the Office refrain from imposing a disclosure requirement in the proposed exemption.

a. A rigid disclosure requirement is unnecessary and would perpetuate the chilling effects of Section 1201 on good-faith security research.

Effective vulnerability disclosure is calculated to mitigate harm to consumers and improve the security of all computing systems by ensuring that security vulnerabilities are fixed, learned from, and disclosed to the public. The best manner and method of achieving these goals depends on a number of situation-specific

[1] Formerly of the Samuelson-Glushko Technology Law and Policy Clinic at Colorado Law.

[2] Initial Comment of Security Researchers at 1; Initial Comment of Dr. Matthew D. Green at 12, 28; Reply Comment of Dr. Matthew D. Green ("Green Reply") at 11-15; Reply Comment of Security Researchers at 1-3.

[3] Copyright Office Hearing on "Library of Congress Sixth Triennial Rulemaking," May 26, 2015, at 131 (Testimony of Christian Troncoso, Business Software Alliance) ("Class 25 Hearing Transcript").

factors.[4] In any given circumstance, a researcher must answer a range of questions to determine how best to disclose a vulnerability: Does the vulnerability affect a single vendor or multiple vendors? Can the vendor(s) be identified and contacted? Is the vulnerability being actively exploited to harm end-users? How should third parties be involved in the disclosure process?[5]

Both researchers and industry agree that appropriate disclosure requires a context-specific inquiry. At the Class 25 hearing, the witness for the Business Software Alliance ("BSA") observed that "the disclosure of vulnerability information must be done judiciously consistent with the facts of the specific situation in ways that avoid unintended consequences."[6] Security researchers agreed, but highlighted the unintended consequences that may flow from good-faith researchers inability to inform other parties and the general public of known vulnerabilities.[7]

An overly complex or rigid disclosure requirement would undermine the very purpose of the proposed security research exemption. In requesting the exemption, researchers are seeking clarity with respect to their ability to perform needed research without seeking permission from the various stakeholders who could threaten liability under Section 1201.[8] Attaching a strict disclosure requirement to the proposed exemption will continue to create uncertainty and risk for security researchers, especially given the complexity involved in making disclosure decisions.

Further, such a requirement is unnecessary. Good-faith security researchers, including several proponents of the proposed exemption, have a strong record of practicing responsible disclosure techniques appropriate to the situation at hand.[9] Numerous published guidelines offer best practices for disclosing security

[4] *See* Green Reply at 12-14.

[5] Relevant third parties include the various national Computer/Cyber Emergency Response Teams (CERTs) such as SEI-CERT, ICS-CERT and US-CERT, that assist researchers, vendors, and end-users in the coordination of vulnerability disclosure and minimization of vulnerability harms.

[6] Class 25 Hearing Transcript at 128:13-17 (Testimony of Christian Troncoso).

[7] *Id*. at 151:17-23 (Testimony of Matt Blaze);155:2-12 (Testimony of Matthew Green); 160:2-22 (Testimony of Steve Bellovin).

[8] Pursuant to Section 1203, "any person injured by a violation of Section 1201" may bring suit to enforce the statute's provisions. 17 U.S.C. § 1203.

[9] For example, Professor Green personally notified the Federal Bureau of Investigation and other critical end-users prior to public disclosure of a serious vulnerability in Secure Socket Layer. Green Reply at 12. Professor Nadia Heninger likewise reached out to more than 60 separate vendors to notify them of a common security flaw she discovered. *See* https://crypto.stanford.edu/RealWorldCrypto/slides/nadia.pdf.

vulnerabilities in a variety of situations.[10] These evolving guidelines accommodate the complexity involved in making disclosure decisions and are based on the combined experience of researchers and vendors dealing with a number of unique circumstances. However, those guidelines are too varied and complex to capture effectively in a qualification to the proposed exemption. Additionally, for any effective notification regime to work, it must foster cooperation among security researchers, manufacturers, developers, and vendors, rather than simply serving as grounds for liability for researchers.

Finally, since the enactment of the DMCA, legal scholars have explored the fundamental tensions between the First Amendment's protection of research and scholarship and the Act's anti-circumvention provision.[11] Those tensions would be greatly exacerbated by restrictions on what researchers may say and when they may say it. The Office should not condition a good-faith security research exemption on an inflexible disclosure requirement that overlooks the highly contextual nature of appropriate disclosure practices or that fails to give security researchers the latitude they need to advance the state of the art, inform other security experts, and protect consumers and vendors alike.

b. The ambiguities of Section 1201(j) make it a poor model for a disclosure requirement

Section 1201(j) is not a serviceable model for a disclosure standard for security research. The requirement to seek authorization from the owner or operator of a computer, system, or network in Section 1201(j)(1) would foreclose not only the dissemination of research results, but also the initiation of the research in the first place. As the Office tacitly acknowledged in the hearing, there is more than one reasonable interpretation of that provision and the Office made clear that it was not yet offering a definitive one.[12]

Aside from the authorization provision in Section 1201(j)(1), Section 1201(j)(3)(A) lists whether or not a discovered vulnerability is "shared directly with the developer of [the relevant] computer, computer system, or computer network" as a factor in

[10] *E.g.* Steve Christey and Chris Wysopal, "Responsible Vulnerability Disclosure Process", Internet Engineering Task Force, 2002, available at https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00; CERT, "Vulnerability Disclosure Policy", available at http://www.cert.org/vulnerability-analysis/vul-disclosure.cfm.

[11] Yochai Benkler, *Free As the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. Rev. 354, 427-29 (1999).

[12] Class 25 Hearing Transcript at 104-05, 118-19.

determining whether Section 1201(j) exempts a particular act of circumvention from liability. As with the authorization provision, this factor is ambiguous and raises many questions:

- Who is the "developer"? Is it the software's vendor, assuming one exists? Is it the software's copyright holder? In the case of collaborative or open source software, which developer or developers must be notified?
- What does "shared directly" mean? Does this preclude interfacing with a third party capable of assisting in the coordinated disclosure of security vulnerabilities such as US-CERT or ICS-CERT?[13] Does it allow public disclosure of the vulnerability after the developer has been notified?
- How does this clause account for situations requiring notice to many parties of a large-scale vulnerability affecting more than a single developer? How does this clause interact with the need to protect the general public by notifying them of unpatched, actively and widely exploited vulnerabilities?

Even assuming clear answers to these questions, the disclosure mapped out in Section 1201(j)(3) is only a single factor in an open-ended list. There is no guarantee that a researcher who complies with specific steps in disclosing her activities to a developer, owner, or operator will be protected by the exemption.

The uncertainty inherent in Section 1201 prompted the Office to grant specific exceptions in 2006 and 2010.[14] Instructively, the Office did not include Section 1201(j)'s disclosure clause in those exemptions.[15] The Office should similarly refrain from including a rigid disclosure requirement in the proposed Class 25 exemption.

2. A security research exemption should not incorporate laws unrelated to copyright.

We agree with the Office that it should not and cannot grant an exemption from laws other than Section 1201 in the instant proceeding.[16] Arguments about the

[13] US Computer Emergency Response Team, https://www.us-cert.gov/; Industrial Control Systems Cyber Emergency Response Team, https://ics-cert.us-cert.gov/.

[14] Exemption to Prohibited Circumvention of Copyright Protection Systems for Access Control Technologies, Final Rule, 71 Fed. Reg. 68472 (Nov. 27 2006) ("2006 Notice"); Exemption to Prohibited Circumvention of Copyright Protection Systems for Access Control Technologies, Final Rule, 75 Fed. Reg. 43825 (July 27 2010) ("2010 Notice").

[15] 2006 Notice at 68477; 2010 Notice at 43832.

[16] Class 25 Hearing Transcript at 204:4-6 ("We will not be granting an exemption that somehow suggests that you can violate other laws.") (Statement of Jacqueline Charlesworth, General Counsel and Associate Register of Copyrights).

consistency of security research with the Clean Air Act, the Computer Fraud and Abuse Act ("CFAA"), trade secret protections, or other laws and regulations are best left to the administrative and law enforcement agencies with the obligation and expertise to interpret and enforce those laws and regulations. Good-faith security researchers strive to follow the law and uniformly condemn the unauthorized malicious hacking of live systems controlling critical infrastructure as neither lawful nor consistent with good faith.[17] But this does not mean that Section 1201 should incorporate either those laws or their remedies.

The CFAA provides an example of the problems inherent in hinging an exemption under Section 1201 on compliance with laws and regulations unrelated to copyright. The scope of liability under the CFAA is unclear and not uniform across judicial circuits.[18] Because Section 1201(j) incorporates the CFAA, whether it protects a researcher's work from liability potentially could turn in part on the particular circuit in which she performs that research. Moreover, the Office is not empowered to resolve inconsistencies or ambiguities in the CFAA or any of the statutes and regulations that opponents have cited in opposing an exemption from liability under the Copyright Act.

In recommending prior security research exemptions, the Office has noted uncertainties in Section 1201(j) that leave insufficient protections for crucial good-faith security research.[19] The Office can substantially limit the uncertainty of any exemption by not expressly incorporating laws and regulations unrelated to copyright. This will not leave researchers exempt from liability under those laws. It will merely avoid compounding the uncertainty and legal risk that researchers currently face under them.[20]

[17] See Class 25 Hearing Transcript at 146:10-18 ("We are very much concerned with avoiding breaking laws.") (Testimony of Steve Bellovin); 150:16-20 (condemning "tampering with live safety, critical systems" and clarifying that "nobody advocates that here") (Testimony of Matt Blaze).

[18] For example, courts have used different analysis and reached different conclusions with respect to the scope of liability under the CFAA for employees. *Compare United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012) (no CFAA liability for violation of a company privacy policy) *with Int'l Airport Ctrs. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006) (employee access to company's computer became unauthorized following breach of duty of loyalty).

[19] *See* 2006 Notice at 68477 (noting uncertainty with respect to whether Section 1201(j) permitting circumvention of TPMs controlling access to sound recordings for purposes of testing those TPMs).

[20] *See* Statement of Legal Impediments to Cybersecurity Research, available at http://www.ischool.berkeley.edu/files/cybersecurity-statement-rev9.pdf.