Before the
U.S. Copyright Office, Library of Congress
Washington, DC

In the Matter of **Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies**	))))	Docket No. 2014–07

Response to Post-Hearing Questions on Proposed Class 25: Security Research

Dr. Matthew D. Green, PhD
Assistant Research Professor
Department of Computer Science
Johns Hopkins Information Security Institute
Johns Hopkins University
mgreen@cs.jhu.edu • 410-861-0344
spar.isi.jhu.edu/~mgreen/
3400 N. Charles Street, 209 Maryland Hall,
Baltimore, MD 21218

Samuelson-Glushko Technology Law & Policy Clinic (TLPC)
Counsel to Prof. Green
Prof. Blake E. Reid, Director
blake.reid@colorado.edu • 303-492-0548
Colorado Law
Robert & Laura Hill Clinical Suite • 404 UCB
Boulder, CO 80309-0404

We appreciate the opportunity to respond to the Office's post-hearing questions regarding the inclusion of a vendor disclosure requirement, including the constitutionality thereof, in the proposed exemption, and how the exemption relates to other laws and statutory provisions. We urge the Office to grant the exemption without a disclosure standard or, in the alternative, to recommend a flexible disclosure carefully crafted to avoid constitutional conflicts and undue interference with the legitimate needs and practices of the research community. We also urge the Office not to narrow the proposed exemption on the basis of its interaction with other laws.

I. A rigid disclosure standard is both unnecessary and constitutionally suspect.

As we have repeatedly noted in this proceeding, a rigid disclosure requirement is unnecessary and inappropriate.[1] Conditioning eligibility for the proposed exemption on such a requirement would serve only to perpetuate Section 1201's current chilling effect on security research by introducing additional complexity and ambiguity surrounding what a good faith security researcher can do.[2] Security researchers, including Prof. Green, already follow best-practice disclosure guidelines and a range of other best-practice standards for good faith security research.[3] Accordingly, a disclosure requirement or restriction is unnecessary, and we strongly oppose the inclusion of such a requirement or limitation.

---

[1] *E.g.*, *Reply Comment of Dr. Matthew D. Green*, at 11-15 ("*Green Reply*"), http://copyright.gov/1201/2015/reply-comments-050115/class%2025/ReplyComments_LongForm_Green_Class25.pdf.
[2] *See Long-Form Comment of Dr. Matthew D. Green*, at 17-19 ("*Green Comment*"), http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_Green_Class25.pdf.
[3] For example, researchers performing their duties in good faith never conduct research on live systems actively protecting critical infrastructure, medical devices while implanted in patients, or vehicles while in use for non-research purposes.

The Office appears to be contemplating both (1) a requirement that researchers notify owners, operators or developers a certain period of time in advance of publicly disclosing security research results and (2) a limitation of what information may be in the public disclosure. Both the requirement and the limitation create significant but distinct tensions with the First Amendment.

A regulation preventing researchers from publicly disclosing a vulnerability until a certain period of time after they disclose the same vulnerability to the owner, operator, or developer of a computer, computer system, or network, would constitute a restriction on protected speech.[4] Even if it were deemed content-neutral (which is by no means certain), such a regulation would need to be narrowly tailored to serve a significant government interest.[5]

In both written comments and oral testimony, we and other researchers made clear that the appropriate timing of disclosure is a fact-specific inquiry to which a bright-line disclosure requirement is ill-suited.[6] Even opponents of the proposed exemption agree. The Business Software Alliance stated that "every vulnerability is different, and the fix to every vulnerability may take a different amount of time."[7] Accordingly, the BSA would be "probably uncomfortable with a fixed deadline for" disclosure.[8] Because both proponents and opponents agree that an inflexible disclosure standard would ill serve the purposes of both security researchers and vendors or owners, such a requirement is unlikely to be appropriately and narrowly tailored to achieve the purpose of protecting both vendors and the public from harm from vulnerabilities.

Aside from the constitutional concerns inherent in a requirement that would give vendors the right to block publication of research results, the Office's suggestion that a restriction should be placed on *what* researchers may publish raises different First Amendment questions. Because such a restriction would aim directly at the content of protected speech, that restriction must be the least restrictive means of achieving a compelling interest to pass First Amendment muster.[9]

Professor Steven Bellovin's hearing testimony made clear that a restriction limiting the details of a known vulnerability that may be disclosed would be unlikely to prevent determined hackers from exploiting a vulnerability.[10] Further, such a restriction would *undermine* the legitimate interest in adequately protecting both vendors and the public against vulnerabilities because it would prohibit sharing the information needed to explain the vulnerability, learn from the exploit, and protect the public.[11] Such a restriction would also be inconsistent with basic tenets of

---

[4] *See Universal City Studios v. Corley*, 273 F.3d 429, 447 (2d Cir. 2001) (noting that "courts have subjected to First Amendment scrutiny restrictions on the dissemination of technical scientific information . . . and scientific research" (internal citations omitted)).

[5] *E.g.*, *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989).

[6] *See* Green Reply at 14 (noting that "the proper manner and method of responsibly disclosing a security vulnerability is a complex and situation-specific task not well suited for codification in a Section 1201 exemption"); *Transcript of Sixth Annual Triennial 1201 Rulemaking Hearings*, May 26, 2015, at 80 ("*Transcript*") (testimony of Matt Blaze) (proper disclosure is "a question that has to be answered on a case-by-case basis"). http://copyright.gov/1201/2015/hearing-transcripts/1201-Rulemaking-Public-Roundtable-05-26-2015.pdf.

[7] *Transcript* at 131 (testimony of Christian Troncoso).

[8] *Id*. at 131-32.

[9] *E.g.*, *Sable Commc'ns of Cal., Inc., v. FCC*, 492 U.S. 115, 126 (1989).

[10] *Transcript* at 193-94 (testimony of Dr. Steven Bellovin) ("'There's a security vulnerability in the tire pressure monitor wireless system.' That statement alone is enough for the serious enemies [to attack the system]—and those are the ones I'm most concerned about—to do it.)

[11] *See id.* at 185 (testimony of Dr. Matt Blaze).

the scientific method, such as the verification of results by reproduction, through which our understanding of *all* vulnerabilities advances.[12]

These constitutional infirmities would be further compounded by attempting to accomplish the asserted legitimate interest through copyright law. As the Ninth Circuit recently held in *Garcia v. Google*, serious threats to privacy, emotional distress, or even life and limb are not cognizable copyright harms because they are too attenuated from the purposes of copyright.[13] Placing disclosure restrictions on a Section 1201 exemption will do little to protect vendors or the public from harms that, at their core, have nothing to do with copyright infringement.

II. If the Office chooses to recommend a disclosure standard, the standard must be flexible enough to accommodate a wide range of scenarios to ensure that public harm does not ensue.

Presuming for the sake of argument that a disclosure requirement could successfully serve a compelling government interest by preventing malicious exploitation of vulnerabilities in some circumstances, such a requirement would need to be sufficiently narrowly tailored to serve that purpose without unduly restricting or burdening a researcher's speech. Because the likelihood that a particular disclosure approach will either lead to or prevent malicious exploitation of the disclosed vulnerability is a complex multi-factor determination, it would be extremely difficult to codify a disclosure requirement that is sufficiently narrowly tailored. Therefore, granting the proposed exemption free and clear of any disclosure requirement is the best way for the Office to avoid constitutional infirmity. Doing so would also avoid the peril of a disclosure requirement that undermines the very purposes it is intended to serve by keeping needed information from those in the best position to assess a vulnerability's severity and take appropriate action.

If the Office nevertheless recommends conditioning the proposed exemption on a disclosure requirement, that requirement must be flexible enough to accommodate the range of situations frequently encountered when notifying affected parties of vulnerabilities discovered in the course of performing good faith security research. These situations include:

- Where a discovered vulnerability is being actively exploited to harm end-users, requiring an immediate public disclosure to mitigate such harm.[14]
- Where multiple works all suffer from the same or related flaws, requiring disclosure coordination amongst multiple entities.[15]
- Where the vendor or responsible party has no interest in addressing or correcting the discovered flaw.[16]

---

[12] *See id*. at 186 (testimony of Dr. Matt Blaze).

[13] *Garcia v. Google, Inc.*, 786 F.3d 733, 744-46 (9th Cir. 2015) (en banc).

[14] For example, this occurred with Common Vulnerability and Exposure (CVE) 2015-0313 involving a vulnerability in Adobe Flash. Symantec, *New Adobe Flash zero-day is being exploited in the wild* (Feb. 2, 2015), http://www.symantec.com/connect/blogs/new-adobe-flash-zero-day-being-exploited-wild.

[15] For example, this occurred with the Heartbleed, Shellshock, and Logjam vulnerabilities. CVE-2014-0160 (Heartbleed), http://heartbleed.com/; CVE-2014-6271 (Shellshock), https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271; CVE-2015-4000 (Logjam), https://weakdh.org/.

[16] For example, this occurs when vendors no longer supporting or patching products, such as Microsoft's Windows XP. Microsoft, *Windows XP support has ended* (last accessed June 29, 2015), http://windows.microsoft.com/en-us/windows/end-support-help.

- Where identifying or contacting the vendor is difficult or impossible.[17]
- Where a researcher bypasses a TPM in order to engage in good faith security research, but then fails to discover any vulnerabilities worth disclosing.[18]
- Where a researcher discovers a vulnerability, but chooses not to disclose it publicly.[19]

Furthermore, the Office must make clear in any disclosure requirement exactly to whom any discovered vulnerability must be disclosed, whether the copyright holder of the vulnerable code, the developer who maintains the vulnerable code, the vendor of software or devices including the vulnerable code, or the software or device end-users directly harmed by the vulnerability, bearing in mind that with many vulnerabilities, the relevant copyright holders, developers and vendors may be numerous and distinct. For example, products including open source libraries or software may have hundreds or even thousands of developers or copyright holders with loose or no affiliation.[20] Failing to account for these details through a sufficiently flexible disclosure requirement would risk restricting essential public disclosure of a vulnerability that might in turn result in harm to the public.

At the same time, attempting to provide the necessary flexibility through a multi-factor approach to disclosure would offer no firm guarantee to researchers that their activities will not subject them to liability or threat of liability under Section 1201 and would fail to address the basic need for certainty upon which the proposed exemption is premised. Indeed, the uncertainty of such multi-factor approaches is one of the principal defects of Section 1201(j) that has made this and other security research exemptions necessary.[21]

Accordingly, should the Office recommend a disclosure requirement, we urge a flexible approach that ensures that any uncertainty about the propriety of any public disclosure errs in favor of allowing the researcher to proceed. Such an approach might modify our proposed exemption language as follows (additions in italics):

> Literary works, including computer programs, databases, and documentation, protected by technological protection measures that control access to the work, for the purpose of finding, fixing, and disclosing security vulnerabilities, flaws, or malfunctions, commenting on or criticizing such vulnerabilities, flaws, or malfunctions, or engaging in scholarship and teaching about such vulnerabilities, flaws, or malfunctions, including where the technological protection measures control access to other works, such as graphic works, audiovisual works, and sound recordings, when the research cannot be performed without accessing the other works*, if a researcher who chooses to publicly disclose a discovered vulnerability, flaw, or malfunction, first makes a good faith effort to notify parties responsible for repairing*

---

[17] For example, this occurs where the vendor is no longer in business, or, as in the case of many open source projects, where a single work may have hundreds of individual rights holders, many of whom can not be contacted.

[18] *See Green Reply* at 14-15.

[19] For example, this may occur when the researcher feels there is no ethically responsible way to disclose. *See Transcript* at 90 (testimony of Dr. Steven Bellovin).

[20] Because Section 1203 of the DMCA allows "[a]ny person injured by a violation of section 1201" to bring suit, requiring a researcher to contact anyone potentially capable of bringing an action under Section 1201 would impose an unadministrable and undue burden—and an undeniable adverse effect—on the researcher. *See* 17 U.S.C. 1203(a).

[21] For example, in many circumstances there is no certainty as to the identity of the owner, operator, or developer to whom disclosure might weigh Section 1201(j)(3)(A)'s disclosure factor in favor of a researcher's eligibility for Section 1201(j)(2)'s exemption.

*software affected by the vulnerability, flaw, or malfunction or for minimizing harm resulting from the vulnerability, flaw, or malfunction prior to disclosing the vulnerability, flaw, or malfunction to the general public, except where end-users or systems are in imminent danger of harm from the vulnerability, flaw, or malfunction or the public interest otherwise weighs against advanced non-public disclosure***.**

III. The Office should decline to narrow the proposed exemption on the basis of its interaction with other laws.

Researchers whose activities would be covered by the proposed exemption are unquestionably committed to ensuring that their work remains consistent with other laws, including the Computer Fraud and Abuse Act. Moreover, we agree with the Office that the grant of an exemption to Section 1201 can neither enlarge nor narrow the scope of conduct permitted under laws *other* than Section 1201.[22]

However, we strongly urge the Office to squarely maintain the focus of this proceeding on the narrow scope of issues cognizable under Section 1201—namely, the impact of circumvention on *copyright infringement.*[23] The record in this proceeding contains scant evidence that any of the activity enabled by the proposed exemption would result in any harm to copyright interests.

Moreover, there is no reason for the Office to intermingle the copyright considerations at issue in this proceeding with other, complex policy considerations unrelated to copyright, such as cybersecurity, environmental protection, medical policy, or aviation safety. While each of those areas warrants serious attention from policymakers, the appropriate context for their consideration is before the agencies responsible for administering relevant laws in those areas. Any attempt to shape policy in those areas through this proceeding would be wholly inappropriate and inconsistent with the delegative principles of administrative law, just as if the agencies tasked with administering those areas sought to influence the contours of copyright law through their unrelated policy portfolios. Other laws exist to address discrete, sector-specific concerns that security research may raise and remedies under those laws will remain available to affected stakeholders.

The proposed exemption would simply make clear that good faith security research is consistent with the copyright considerations that Section 1201 aims to protect. To grant the exemption, the Office need only affirm that good faith security research is consistent with Section 1201, as the record in this proceeding conclusively demonstrates.

Respectfully submitted,

/s/

Dr. Matthew D. Green

Prof. Blake E. Reid
Counsel to Prof. Green

---

[22] *Transcript* at 204 (Statement of Jacqueline Charlesworth).

[23] *See* discussion, *supra*, at 3 & n.13 (noting the constitutional problems inherent in enforcing non-copyright interests with copyright law).