Prof. Andrea Matwyshyn
Princeton University
305 Sherrerd Hall
Princeton, NJ 08544
am28@princeton.edu

On behalf of herself and

Prof. Steve Bellovin
Columbia University
454 Computer Science Building
1214 Amsterdam Avenue M.C. 0401
New York, NY 10027

Prof. Matthew Blaze
University of Pennsylvania
220 South 33rd Street
107 Towne Building
Philadelphia, PA 19104

Mark Stanislav
Rapid7
100 Summer Street, 13th Floor
Boston, MA 02110

June 29, 2015

Hon. Jacqueline C. Charlesworth
General Counsel and
Associate Register of Copyrights
2015admat@loc.gov

Re: Docket No. 2014-7 Exemptions to Prohibition Against Circumvention of Technological Measures Protecting Copyrighted Works

Dear Associate Register Charlesworth:

In response to the follow-up questions posited by the Copyright Office with respect to Proposed Class 25–Software–security research as part of the Copyright Office's Section 1201 rulemaking proceeding, we respectfully submit the following information:

1. ***Given concerns raised by participants regarding disclosure of research results to manufacturers, please provide any additional thoughts you may have as to how the Office might approach this issue if it were to recommend the requested exemption. If some sort of disclosure to the manufacturer were required, what would that process be? Please address any relevant First Amendment or regulatory issues in your response.***

    a. <u>The proposed exemption process</u>

With respect to the formulation of a proposed exemption, we reiterate the position articulated in our prior filing. If some sort of disclosure to the manufacturer whose product or service was the primary subject of research is required, an exemption should be crafted in the following manner:

" Literary works, including computer programs and databases, protected by access control mechanisms that potentially expose the public to risk of harm due to malfunction, security flaws or vulnerabilities when

(a) circumvention is accomplished for the purpose of good faith testing for, investigating, or correcting such malfunction, security flaws or vulnerabilities in a technological protection measure or the underlying work it protects; OR

(b) circumvention was part of the testing or investigation into a malfunction, security flaw or vulnerability that resulted in the public dissemination of security research when (1) a copyright holder whose works were used fails to comply with Reasonable Vulnerability Management Practices; or (2) the finder of the malfunction, security flaw or vulnerability reports the malfunction, security flaw or vulnerability to the copyright holder whose works were used by providing Vulnerability Replication Information in advance of or concurrently with public dissemination of the security research.

For purposes of this exemption,

<u>Reasonable Vulnerability Management Practices</u> shall be defined as the following requirements, which mirror those appearing in ISO 29147 and 30111:

1. Creation and prominent publication of a publicly-viewable corporate vulnerability disclosure policy on the corporate website.
2. Creation and prominent display of a prominent internet "front door" – clear instructions for submitting external vulnerability reports to the company on the corporate website.
3. Creation of an internal corporate vulnerability management handling process which designates responsible individual(s) for (1) intake, handling, monitoring of public sources for vulnerability information and (2) external finder communications, who possess(es) adequate corporate authority to bind the company in its promises to finders.
4. Acknowledgement of all external reports of malfunctions, security flaws or vulnerabilities within seven calendar days of a finder's submission.

Vulnerability Replication Information shall be defined as the following items, which mirror those in Annex A of ISO 29147:

1. a basic summary that includes (a) a technical description, (b) the finder's contact information, (c) a description of any public disclosure plans known as of the day of alerting the copyright holder to the vulnerability, (c) projected impact or a threat and risk assessment, to the extent possible (d) a description of the software configuration at the time of the discovery, if not default; (e) any relevant information about connected devices; AND

2. a product-specific component consisting of (a) if the software or hardware, the product name or model, the operating system, and the version or revision number of the product or (b) if an online service, the time and date of discovery, the relevant URL, browser information including type and version, and the input required to reproduce the vulnerability."

This formulation creates a fair balance between providing notice to a copyright holder whose products or services were the direct subject of the research and the protected First Amendment speech of a researcher.

b. First Amendment protection for researcher publication of vulnerability information

Courts will deem the First Amendment to fully protect the speech of a security researcher who seeks to advance information security discourse through presentation of research results using a reputable channel, such as a conference presentation or academic journal, particularly when the researcher has engaged in obvious harm mitigation measures.[1] The Security Researchers' exemption request was crafted with this First Amendment reality in mind.

Let us imagine a case where a vendor sues an academic researcher under the DMCA (or CFAA) for publishing an article in conference proceedings disclosing the existence of a serious security vulnerability in a particular category of product, naming the product used to discover the security flaw. Courts will analyze the question of whether the First Amendment bars such a claim in one of two ways. Some courts are likely to immediately deem the speech to be obviously First Amendment protected on its face, rendering the claim not viable.

Other courts may, more conservatively, entertain the argument that the speech is dual purpose "instructional" or "informational" speech. In other words, the plaintiff will argue that the speech might cause harm if it is maliciously repurposed by others, and that this potential repurposing justifies its suppression and punishment. The plaintiff will argue that because of these incidental harms at the hands of third parties other than the speaker, the speech should be suppressed and

[1] For example, in connection with such a publication, the researcher might contact the author of the flawed code, describe mitigations in the published work or withhold details of the exploitation of the vulnerability that would be of use only to malicious actors. For a more thorough discussion of the First Amendment analysis of vulnerability speech *see* Andrea M. Matwyshyn, *Hacking Speech: Informational Speech and the First Amendment*, 107 Nw. U. L. Rev. 795 (2013).

the First Amendment does not present a bar to the claim. However, this argument is unsupported by the current state of First Amendment caselaw and will fail.

Even if the researcher's speech in question is classified by courts as informational speech, it will nevertheless be deemed First Amendment protected.[2] Specifically, courts will turn to *U.S. v. O'Brien*[3] for analytic guidance regarding whether the alleged statutory basis for suit constitutes a prior restraint that violates the First Amendment. *O'Brien* dictates that when speech and nonspeech elements are combined in a law potentially impacting speech, courts must assess whether the impact on speech is only incidental or whether the content of communications is implicated. Thus, the intent of the speaker is relevant to a First Amendment analysis of whether informational speech is protected – whether it is a case where "the person engaging in the conduct intends thereby to express an idea." [4] The security researcher in question clearly intends to express an idea: s/he intends to further academic and social discourse around information security. As such, punishing the speech at issue is a case of regulating the communicative aspect of the speech and the content of the speech – an impermissible constitutional overreach. Such a legal sanction would reflect a statutory restriction on First Amendment freedoms that is greater than essential to the furtherance of the asserted interest.[5] In fact, such a claim would be *counterproductive* to any asserted governmental interest in information security: as the numerous Congressional proposals for security information sharing legislation attest, improving information security in our society requires that more information security research be conducted and shared among and by experts.[6] As such, the plaintiff's case would, again, likely be deemed limited by the First Amendment.

---

[2] *Id.* at 832.

[3] The O'Brien test refers to the test set forth by the Supreme Court for expressive conduct in *United States v. O'Brien*, 391 U.S. 367 (1968). In *O'Brien*, the Supreme Court addressed the issue of whether a regulation prohibiting the burning of draft cards constituted a prior restraint on speech that violated the First Amendment. *Id.* at 370–72. The Court determined that "when 'speech' and 'nonspeech' elements are combined in the same course of conduct," only "a sufficiently important governmental interest in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms." Id. at 376.

[4] *O'Brien* at 178.

[5] *Id.*

[6] Specifically, *O'Brien*, therefore, dictates that courts conduct an intent assessment. First, the courts will ask for the subjective perspective of the speaker regarding whether the communication was intended to further discourse or further criminality. *See, e.g. Rice v. Paladin Enters., Inc.*, 128 F.3d 233 (4th Cir. 1997) (Court highlighted that defendant stipulated criminal intent in informational speech that merely aggregated existing murder methodology information). The researcher will state clearly that the subjective intent of the disclosure was furthering public discourse on information security through providing new, important research insights – intent consistent with full First Amendment protection. Next, the courts will assess intent from an objective perspective assessing the researcher's conduct, looking for evidence of communication using due care. *See, e.g., Herceg v. Hustler Magazine, Inc.*, 814 F.2d 1017, 1018 (5th Cir. 1987). (Fifth Circuit found that the First Amendment shielded Hustler Magazine from

2. ***Please briefly address how the proposed exemption might relate to or be limited by other federal or state laws or regulations, including but not limited to the Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030, and any other statutory or regulatory provisions.***

The Security Researchers' proposed exemption request was drafted in an intentionally minimally-disruptive manner by a team of leading academics with significant government service experience across multiple government agencies. The drafting consciously avoids negatively impacting the work of other agencies, and it embraces the evolution of corporate best practices in information security. The proposed exemption would in no way impinge on the ability of the Department of Justice to bring prosecutions under the Computer Fraud and Abuse Act or any other statute, nor would it hamper the enforcement activity of any agency. In fact, it very consciously provides other agencies with breathing room to address information security in the context of their own legal regimes.

Additionally, granting this exemption as requested -- as arising out of DMCA Section 1201(i) – would create an improved legal climate for security research and, therefore, directly facilitate the work of other agencies. As the recent OPM breach clearly demonstrates, agencies are struggling to keep up with information security and need good information from researchers about which products and services are vulnerable to compromise and are likely to expose agencies, their employees, and the national security information they protect to risk. Agencies need more security research information flowing out of the private sector to guide their purchasing and enforcement decisions, not less. Granting this exemption would help to create a stronger flow of information regarding vulnerable products and services both for agencies who need the information to protect federal employee information, such as OPM, and for agencies engaged in

---

liability for informational speech about how to cause death because of defendant's affirmative mitigation measures.) The court will objectively assess whether forum the researcher selected for the speech is a reputable public forum that would be expected to further social discourse on information security. Courts will likely also verify the expressive contribution of the information - is the speech, in fact, furthering the state of knowledge in information security and being disclosed to an audience that shares that goal. A researcher who shares research in a conference proceeding or journal article is certainly doing so in a reputable forum that is consonant with the stated expressive goal: the researcher's behavior is the behavior of someone whose security vulnerability disclosure is intended to help make society safer. Finally, the court will ask whether the researcher engaged in any mitigation measures to avoid criminal repurposing of the vulnerability disclosure. In a case where the speaker considered and actively sought to minimize likely negative incidental effects that would result from the speech, the conduct is again consistent with the intent of furthering public discourse on information security. For an in-depth explanation of this intent analysis, *see* Andrea M. Matwyshyn, *Hacking Speech: Informational Speech and the First Amendment*, 107 Nw. U. L. Rev. 795 (2013).

information security enforcement with respect to consumer products and corporate conduct, such as the FTC, FCC, FDA and SEC.

However, expressly referencing the CFAA in any granted exemption would be highly counterproductive, further chill research, and put undue pressure on the Department of Justice to quickly resolve three existing CFAA circuit splits. In particular, making an exemption grant contingent on the CFAA would immediately and undesirably import the legal uncertainty of the current circuit split on whether a contract breach provides the basis for a CFAA prosecution.[7] As such, referencing the CFAA in an exemption will make the state of security research under the DMCA even more uncertain than it is at present.

An exemption circumscribed by the CFAA is likely to be perceived by security researchers to be confusing and potentially even more hostile to their work than the current legal climate. Similarly, an exemption expressly referencing the CFAA will likely embolden litigious, vulnerable plaintiffs in their frivolous strike suits seeking to silence security research about security inadequacies. Dampening these suits and the damage they cause to national security was the primary impetus for the Security Researchers' exemption request.

.

[7] For a discussion of the state of legal uncertainty regarding the circuit split on contract breach as a basis for CFAA enforcement, *see, e.g.*, Andrea M. Matwyshyn, *The Law of the Zebra*, 28 BERKELEY TECH. L.J. (2013).