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

Petition for Exemption: Applied Cryptography, Security, and Reverse Engineering Research

of

Dr. Matthew D. Green

1. *Submitter and Contact Information:*

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
Christopher E. Meier, Student Attorney
Bridgett Y. Murphy, Student Attorney
Amber L. Williams, Student Attorney
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

Matthew D. Green is a noted cryptography researcher and an assistant research professor at Johns Hopkins University, where he focuses on applied cryptography and cryptographic engineering. Additionally, he investigates how cryptography can enhance user privacy. The student attorneys at the Samuelson-Glushko Technology & Policy Law Clinic (TLPC) at Colorado Law advocate for the public interest in important public policy and legal matters with technological dimensions.

2. *Brief Overview of Proposed Exemption:* Applied Cryptography, Security, and Reverse Engineering Research

This proposed exemption would allow researchers to fortify and improve the cybersecurity of Internet-connected programs, software, and devices—including those that comprise the Internet of Things—to better protect Americans from vulnerabilities that might expose their information and inflict personal or economic harm. For example, this exemption would clear researchers to identify, disclose, and fix security flaws or vulnerabilities in automobile systems, insulin pumps, email systems, and cloud-based storage services, among others.

3. *Copyrighted Works Sought to be Accessed:* Lawfully Obtained Computer Programs and Software, a Subcategory of Literary Works

We tentatively propose an exemption for:

> Computer programs and software, a subcategory of literary works, accessible on personal computers and personal devices and protected by technological protection measures ("TPMs") that control access to lawfully obtained works when circumvention is accomplished for the purposes of good faith testing, investigating, or correcting security flaws and vulnerabilities, commentary, criticism, scholarship, or teaching.

Examples of works within the scope of our proposed exemption include:

- Cryptographic libraries—compilations of cryptographic algorithms used to encipher and decipher messages;
- Malware—software that is used to either disrupt a computer's operation, gain access to private systems, or gather sensitive or private information; and
- Other types of programs or software accessible on personal computers and devices that contain vulnerabilities or security flaws that could potentially harm American consumers, infrastructure, or otherwise pose a threat to cybersecurity.

It is critical that the Librarian adopt a flexible exemption that frees researchers to address evolving security vulnerabilities in a variety of existing and new software over the next three years. We look forward to working with the Office, the National Telecommunications and Information Administration, and other stakeholders to refine the specific contours of this proposed exemption language consistent with the principles laid out in this petition.

4. *Technological Protection Measures:* Technological Protection Measures on Computer Programs or Software that Prevent or Hinder Research in Cryptography, Security, or Reverse Engineering

To access legitimately obtained copies of computer programs or software, researchers will need to circumvent at least one of the following three types of software mechanisms in order to perform good faith security research:

- Software features, such as code obfuscation and runtime checks, that prevent tampering with, changing, or reverse engineering the software;
- Access control checks, such as password or identification code prompts; and

- Encryption, which can serve to conceal the details of security vulnerabilities.

These mechanisms are highly individualized and may not qualify as TPMs under the meaning of 17 U.S.C. § 1201. In many cases, however, we are concerned that these software mechanisms may be characterized as TPMs by entities seeking to chill legitimate, good faith security research by asserting claims under Section 1201.

5. *Noninfringing Uses:* Engaging in Good Faith Computer Security Research to Investigate Security Flaws and Vulnerabilities in a Computer Program or Software

Good faith computer security research comprises a variety of non-infringing activities that either do not constitute copyright infringement or are paradigmatic fair uses under 17 U.S.C. § 107:

- *Researching and discovering security flaws and vulnerabilities*. By investigating and discovering security flaws and vulnerabilities in computer programs or software in good faith, legitimate computer security researchers engage in scholarship or research.
- *Alerting consumers and notifying companies of security flaws and vulnerabilities*. Legitimate computer security researchers who document and responsibly disclose security flaws and vulnerabilities of a software or its mechanisms engage in criticism, commentary, and news reporting by alerting consumers and notifying companies of actual or potential security problems.
- *Providing students with valuable learning opportunities to gain hands-on experience by working on a real system*. In a computer lab setting, professors who permit students to investigate software security flaws and vulnerabilities engage in teaching because students receive an educational benefit from the hands-on experience that they might not otherwise receive.
- *Contributing to the academic publications and discussions of computer program and software security*. Legitimate computer security researchers investigating security flaws and vulnerabilities in good faith engage in scholarship and research that constitute transformative fair uses because they contribute their scientific findings to academic publications and discussions of computer and software security.
- *Applying research discoveries to build a new, secure computer program or software*. Finally, legitimate computer researchers engage in fair use when they apply what they have learned to build a new, secure computer program or software to fix security flaws in an existing program or software.

6. *Adverse Effects:* Chilling Effects on Cryptography Researchers and Negative Impacts on Cybersecurity

Academic and amateur cryptography researchers, commonly known as “white hat” researchers, are adversely affected by Section 1201 in their research because they are in constant danger of burdensome and costly litigation, both threatened and real. They operate in an environment of high risk and low predictability and fear that their scientific and academic work will be subjected to legal challenge under Section 1201, which may threatens their academic freedom, their right to speak freely under the First Amendment, and their jobs. As a result, many legitimate research projects that would boost cybersecurity never get off the ground.

While some good faith security research is already covered by existing exemptions in 17 U.S.C. § 1201(f), (g), and (j) for reverse engineering, encryption research, and security testing, ambiguities in and burdensome requirements to qualify for those exemptions warrant the broader exemption we propose here. For example, these provisions include complex multifactor tests that cannot be evaluated *ex ante*, potential restrictions on the dissemination of research results, and requirements to seek authorization in advance of performing research. While the existing exemptions afford some relief, a broader exemption would ensure that Section 1201 does not interfere with critical security research or hinder the cybersecurity of critical information infrastructures—a critical national priority.

Americans not only face financial harm from these burdens on good faith security testing, they face real threats of physical and financial harm. The automotive industry increasingly relies on computer systems to control the cars of the future; everything from the throttle control, to the brakes, to the door locks, relies on potentially vulnerable software. Medical devices like insulin pumps, pacemakers, hearing aids, and respiratory devices depend on software that can be attacked. Giving white hat researchers greater freedom to identify and help fix vulnerabilities will increase the security of these technologies as new shortcomings are identified.

Finally, the absence of a broader exemption for good faith security research serves to aid malicious "black hat" hackers who operate in secret and are undeterred by Section 1201's provisions. In the absence of legal avenues for conducting legitimate cryptography research, more security flaws exist in computer programs and software that can be exploited by black hat hackers. If legitimate security researchers are able to help identify and fix security vulnerabilities before black hats are able to exploit them, then malicious hacking would become increasingly difficult. Opening additional legal avenues for legitimate security researchers will afford black hat hackers an incentive to responsibly disclose and help fix the vulnerabilities they discover rather than selling them to foreign governments, multinational corporations, or criminal elements.

Respectfully submitted,

/s/

Blake E. Reid
Counsel to Prof. Green

blake.reid@colorado.edu
303.492.0548

Christopher E. Meier, Student Attorney
Bridgett Y. Murphy, Student Attorney
Amber L. Williams, Student Attorney