Short Comment Regarding a Proposed Exemption
Under 17 U.S.C. 1201

Commenter Information

Dr. Matthew D. Green, PhD, is an Assistant Research Professor in the Department of Computer Science at Johns Hopkins University. He is represented by the Samuelson-Glushko Technology Law & Policy Clinic (TLPC) at the University of Colorado Law School, including Chelsea E. Brooks, Student Attorney, Joseph N. de Raismes, Student Attorney, Andy J. Sayler, Student Technologist, and Prof. Blake E. Reid, TLPC Director.

Proposed Class Addressed

Proposed Class 22: Vehicle Software—Security and Safety Research

Statement Regarding Proposed Exemption

Modern vehicles are increasingly controlled by software systems. As such, the security of this software is critical to the safety of vehicle operators, those they transport, and anyone in the proximity of such vehicles. Unfortunately, there are well-documented cases of security vulnerabilities in many of today's vehicles, some of which could lead to life-threating accidents if exploited: for example, flaws allowing attackers to disable a vehicles breaks or steering while a vehicle is moving at speed.[1] It is thus extremely important that security researchers are able to undertake good faith studies of vehicle software with an aim at finding, disclosing, and fixing such vulnerabilities without fear of prosecution under Section 1201. Today, the ambiguity and onerousness of the current security-related DMCA exemptions impose a high degree of risk, overhead, and uncertainty on researchers, chilling security research and necessitating a clearer exemption.

While we support this exemption, we also feel that good faith security research must be allowed on a range of works much broader than vehicle software alone. Beyond vehicles, there exists a huge range of devices and software critical to the security of individuals and our nation: for example, communication systems, medical devices, and power systems. As such, we believe that granting a broad good faith security exemption as proposed in Class 25, covering all forms of devices and software, is the best solution to ensuring that researchers may work unhindered to improve the safety and security of the digital systems on which we all rely. Such an exemption is in line with the broad, but unfortunately unclear, statutory exemptions Congress included in Section 1201. Rather than continuing to grant piecemeal security exemptions for specific sub-classes of works, the Copyright Office should honor Congressional intent by granting a broad exemption for all forms of good faith security research.

[1] Stephen Checkoway, *et. al.*, *Comprehensive Experimental Analysis of Automotive Attack Surfaces*, USENIX Security, 2011. Charlie Miller and Chris Valasek, A Survey of Remote Automotive Attack Surfaces, Black Hat, 2014.