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 27: Software—Networked Medical Devices

Statement Regarding Proposed Exemption

Medical devices are one of the clearest examples of software being directly linked to the livelihood and safety of an individual. As such, it is of the utmost importance that such devices are secure and free from vulnerabilities that might be exploited by malicious actors to harm or kill their users. Unfortunately, there are well-documented cases of security vulnerabilities in a range of existing medical devices, from pacemakers to insulin pumps.[1] It is thus extremely important that security researchers are able to undertake good faith studies of networked medical devises 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 networked medical devices alone. Beyond medical devises, there exists a huge range of devices and software critical to the security of individuals and our nation: *e.g.* communication systems, vehicles, power systems, etc. 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] Daniel Halperin, et. al., *Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses*, IEEE Symposium on Security and Privacy, 2008; Jerome Radcliffe, *Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System*, Black Hat 2011, Los Vegas, NV.