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

Item 1. Commenter Information

Jay Radcliffe, Senior Security Consultant, Rapid 7

Item 2. Proposed Class Addressed

Proposed Class 25: Software—Security Research

Item 3. Statement Regarding Proposed Exemption

As a security research professional with expertise in medical device research and as an insulin dependent Type 1 diabetic, I strongly urge the Copyright Office to grant the security research exemption proposed by the Security Researchers under Class 25. The DMCA has damaged both my research and my quality of life as a diabetic. I have refrained from performing research on firmware in medical devices because of my fear of legal consequences under the DMCA. This research that I have not performed based on the advice of my attorney includes research on the following code-dependent devices that have the capacity to kill or injure patients through malfunction: (1) Insulin pumps, including the Animas Ping, T-Slim, Dexcom and G4, (2) Artificial organs, including the Medtronic Artificial Pancreas, (3) Birth control implants; (4) Kidney dialysis machines; (5) Morphine infusion pumps; and (6) Smart contact lenses for diabetes monitoring.

Because of the DMCA, as much as 40% of the computer code in these medical devices remains untested for safety by independent security experts. I am confident that I would find serious flaws in some or all of these devices if the DMCA did not prevent my research. Because of this lack of safety research, as a type 1 diabetic, I feel that using an insulin pump is too unsafe, and I instead self-inject with needles many times daily. I am not alone in this safety assessment: other diabetic security researchers behave similarly. However, children who need more precise insulin dosing than I do, do not have the option or skill to self-inject. In other words, the DMCA's prohibition on firmware research is actively making diabetic children, in particular, less safe.

No negative repercussions will arise with respect to the safety or security of software from granting this exemption. To the contrary, if the exemption is granted, security researchers will be better able to find existing problems and make all patients safer. To the extent that security issues currently exist, we want them to be found by "good-guy" security researchers. Currently the chilling effect of the DMCA gives the "bad-guy" researchers an advantage. Patients like me deserve the best possible information about the safety of the life-saving devices we need. While a small percentage of outdated devices may suffer from "forever-day" vulnerabilities, meaning security vulnerabilities that supposedly cannot be fixed or patched, the good news is that these problems are increasingly rare: these unsafe devices are being phased out by responsible companies and replaced. I have personally been involved in these types of cases, as a patient and as a researcher. The technology now exists for medical devices to be updated without invasive surgery. In fact, most implanted medical devices can have their settings changed remotely in minutes with no risk to the patient. If a machine or device still exists that cannot be updated, it is fatally flawed in design and too unsafe for human use. It should be replaced as soon as possible. Also, the possible existence of such a serious design flaw highlights the urgent need for more security research, not less. The security research that has been done in traditional computer systems has helped manufacturers cumulatively learn to design systems that can be easily updated to quickly address vulnerabilities. More security research is the time-proven remedy to substantially improve design from the ground up and reduce the number of systems that could have a serious flaw or vulnerability due to bad design. Allowing more security research to be done will help provide safer medical devices for patients with each generation of their medical device. Please grant this exemption, and let me help make the devices that patients like me need safer.