

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

Item 1. Commenter Information

Mark Stanislav, Senior Security Consultant and Researcher, Rapid7

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 Internet of Things device research, 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: in the past the DMCA has been wielded as a weapon against me by companies that were unreceptive to my attempts to engage with them to confidentially disclose and help fix security flaws that I found in products for use by small children. I am not alone in this experience. The act of analyzing firmware to verify its safety for consumer use often lands a researcher like me in a legal nightmare. It could even be enough to end a bright research career unless you are willing to endure a lengthy court battle.

Many of the technologies that consumers buy have no real assurances that they adequately protect our privacy as the device's box may claim. There aren't rigorous security checks before a consumer can buy a nursery web camera off the shelf or any audit of the programming done before an Internet-connected toy is placed into the hands of a small child. Instead, consumers are left to blindly trust the vendor of the product that they've done all reasonable security audits to protect us. In my own research with these two sets of products—web cameras and Internet-connected children's toys—I have seen real, horrifying examples of a gratuitous lack of security. Unfortunately, we in the security research community find such defects frequently. My own research addressed issues in these contexts and provided resolution to critical flaws that would have otherwise put thousands of families and children at risk for invasion of their privacy or even enable child predators to anonymously contact a small child over the Internet.

Security researchers want to use our skills to help protect the privacy and safety of citizens and our country. But, because of the DMCA, legal risk dramatically curtails the research that security researchers are willing to undertake. Through my own legal scares over the years with companies who would rather involve lawyers and the DMCA than improve the security of their products, I've had to limit the amount of good I can do to help protect consumers. With revolutions such as the Internet of Things well underway, the number of devices going into the personal lives of citizens far out numbers the capacity of the security researchers willing to take great personal legal risks to protect people using those products. As my attempt to mitigate my DMCA legal risk while still improve the dramatic IoT security deficits, I created an initiative called "Build It Securely" to facilitate collaboration between security-aware IoT product vendors and security researchers. Unfortunately, this effort doesn't scale, and the vendors we are able to convince to participate in our initiative are the exception to the rule – they already care about security. The vendors with the most vulnerable products often don't.

While the DMCA certainly has an intention to provide protections for our country's technology interests, it has unfortunately ended up being a huge impediment for those who want to help make that technology safer and help it to avoid compromising the privacy of consumers. The security research exemption proposed by the Security Researchers would allow security researchers to do crucial work to help protect the safety of vulnerable users, particularly children. We will never be able to protect every device or catch every bug, but right now, we're handicapped by the DMCA. Please help change that and grant the exemption request.