Jun. 23, 2021

We the undersigned write to caution against use of Section 1201 of the Digital Millennium Copyright Act (DMCA) to suppress software and tools used for good faith cybersecurity research. Security and encryption researchers help build a safer future for all of us by identifying vulnerabilities in digital technologies and raising awareness so those vulnerabilities can be mitigated. Indeed, some of the most critical cybersecurity flaws of the last decade, like Heartbleed, Shellshock, and DROWN, have been discovered by independent security researchers.

However, too many legitimate researchers face serious legal challenges that prevent or inhibit their work. One of these critical legal challenges comes from provisions of the DMCA that prohibit providing technologies, tools, or services to the public that circumvent technological protection measures (such as bypassing shared default credentials, weak encryption, etc.) to access copyrighted software without the permission of the software owner. 17 USC 1201(a)(2), (b). This creates a risk of private lawsuits and criminal penalties for independent organizations that provide technologies to researchers that can help strengthen software security and protect users. Security research on devices, which is vital to increasing the safety and security of people around the world, often requires these technologies to be effective.

Good faith security researchers depend on these tools to test security flaws and vulnerabilities in software, not to infringe on copyright. While Sec. 1201(j) purports to provide an exemption for good faith security testing, including using technological means, the exemption is both too narrow and too vague. Most critically, 1201(j)'s accommodation for using, developing or sharing security testing tools is similarly confined; the tool must be for the "sole purpose" of security testing, and not otherwise violate the DMCA's prohibition against providing circumvention tools.

If security researchers must obtain permission from the software vendor to use third-party security tools, this significantly hinders the independence and ability of researchers to test the security of software without any conflict of interest. In addition, it would be unrealistic, burdensome, and risky to require each security researcher to create their own bespoke security testing technologies.

We, the undersigned, believe that legal threats against the creation of tools that let people conduct security research actively harm our cybersecurity. DMCA Section 1201 should be used in such circumstances with great caution and in consideration of broader security concerns, not just for competitive economic advantage. We urge policymakers and legislators to reform Section 1201 to allow security research tools to

be provided and used for good faith security research In addition, we urge companies and prosecutors to refrain from using Section 1201 to unnecessarily target tools used for security research.

Bishop Fox
Bitwatcher
Black Hills Information Security
Bugcrowd
Cybereason
Cybersecurity Coalition
Digital Ocean
disclose.io
Electronic Frontier Foundation
Grand Idea Studio
GRIMM
HackerOne
Hex-Rays
iFixIt
Luta Security
McAfee
NCC Group
NowSecure
Rapid7
Red Siege
SANS Technology Institute
SCYTHE
Social Exploits LLC