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

Item A. Commenter Information

USACM is the U.S. Public Policy Council of ACM. The Association for Computing Machinery (ACM) is the world's oldest and largest membership society for technology and computing professionals, with more than six decades of leadership within the computing community. USACM provides independent, nonpartisan, and technology-neutral resources to policy leaders, stakeholders, and the public about public policy. USACM's contributions to public policy are drawn from the deep technical expertise of the computing community.

The membership of USACM includes many experts on computer security who perform research that benefits public safety and welfare, working in both public sector and private sector settings.

Item B. Proposed Class Addressed

We write to **support** a DMCA exemption for ***Proposed Class 10: Computer Programs—Security Research***.

Item C. Statement Regarding Proposed Exemption

Computer security plays an indispensable role in maintaining national security, continuity of operations for mission critical infrastructure (e.g., the power grid, air traffic control), safety of automotive and avionics systems, the integrity of financial transactions, proper operation of medical and consumer devices, business operations, maintenance of personal privacy, and the overall stability of the U.S. economy. Computer security will only become more critical as we see increasing deployment of the "Internet of Things."

Security research is critical to maintaining the security of existing systems, and must be protected and encouraged to further develop and insure such security going forward.

We support the proposed expansion of the current security research exemption for computer software, as proposed by Professors Felten and Halderman.[1] Each of the limitations in the renewed exemption potentially limit the scope and effectiveness of software security research.

Specifically, the limitation by category of device to consumer devices, land vehicles, and medical devices addressed by proposal (1) leaves out emerging security threats to systems outside of this scope, such as commercial drones and building environment and physical security systems.[2] There is no reason to enumerate specific categories at all, given that software technology and internet connectivity are increasingly ubiquitous, and it's difficult to know exactly what new threats may arise.

[1] Petition for New Exemption Under 17 U.S.C. § 1201, Prof. Ed Felten and Prof. J. Alex Halderman, https://www.regulations.gov/document?D=COLC-2017-0007-0056.

[2] Mark Pitchford, "What's needed to ensure safety and security in UAV software," in *Military Embedded Systems*, July 31, 2013, http://mil-embedded.com/articles/whats-needed-ensure-safety-security-uav-software/, and Antone Gonsalves, "Building control systems can be pathway to Target-like attack," *CSO*, Feb. 6, 2014, https://www.csoonline.com/article/2134368/fraud-prevention/building-control-systems-can-be-pathway-to-target-like-attack.html.

Proposals (2-5) address limitations that chill research and innovation by extending beyond infringement prevention, or limiting the rights of researchers.

Detection and correction of security deficits has long been provided by technology professionals, in a broad-based, largely voluntary effort to report software flaws detected during the acquisition, deployment, and operation of software systems. One example is the voluntary reporting system managed by the US-CERT (United States Computer Emergency Readiness Team) at the Department of Homeland Security.

The additional detection and correction of security flaws is regularly performed by those who purchase, install, and operate systems, and by computer professionals who are retained to perform the full arsenal of computer security testing activities. Often those who detect security flaws must immediately repair those flaws to maintain operational security for their systems, and then often return or contribute those “patches” back to the original software providers.

Examination and circumvention are part of this work – and the DMCA creates civil and criminal liability. A perceived association with the DMCA can chill legitimate research – potentially leaving computing systems vulnerable to attack.[3]

In our professional judgment, as computer and computer security professionals, we believe that the security of government and corporate systems, safety of consumer products, security of financial transactions, and even our national security are placed at significant risk if security research and testing is prevented by the threat of prosecution under the DMCA. We strongly urge the Copyright Office to grant this exemption request.

[3] Petition for Proposed Exemption Under 17 U.S.C. § 1201, Steven Bellovin, et al, November 2014, http://copyright.gov/1201/2014/petitions/Bellovin_1201_Intial_Submission_2014.pdf.