March 27, 2015

Library of Congress
Copyright Office
101 Independence Avenue, SE
Washington, DC 20559-6000

RE: In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. 1201—Sixth Triennial DMCA Rulemaking – Proposed Class 25

To the Librarian of Congress and the Register of Copyrights:

The Intellectual Property Owners Association ("IPO") respectfully submits these comments in connection with the sixth triennial rulemaking proceeding under the Digital Millennium Copyright Act ("DMCA"), in opposition to proposed Class 25 covering "Software – security research."

IPO is a trade association representing companies and individuals in all industries and fields of technology who own or are interested in intellectual property rights. IPO's membership includes more than 200 companies and more than 12,000 individuals who are involved in the association, either through their companies or through other classes of membership.

The petition to circumvent the technological protection measures (TPMs) in class 25 should be denied because it is over broad and would create significant public risk.

The requested exemption for proposed class 25 "would allow researchers to circumvent access controls in relation to computer programs, databases, and devices for purposes of good-faith testing, identifying, disclosing, and fixing of malfunctions, security flaws, or vulnerabilities." Proponents argue the exemption is needed "across a wide range of systems and devices." That wide range includes not only medical devices and smartphone applications that operate those devices, but also car components, supervisory control and data acquisition systems, and other critical infrastructure, such as the computer code that controls nuclear power plants, smartgrids, and industrial control systems, internet-enabled consumer goods in the home, and transit systems. In view of the vast array of products that could be accessed through the exemption, the public risk is impossible to quantify.

Regarding circumvention of TPMs in medical devices and smartphones that operate critical applications for those devices, such as pacemaker applications, for the stated purpose of "fixing … malfunctions, security flaws, or vulnerabilities" no one should be "fixing" medical devices or pacemaker applications without Food and Drug Administration ("FDA") review and approval. The risk of patient injury or death is high.

Second, there is risk associated with disclosing software for these devices and applications prior to FDA review and approval. Due to the length of the development and review process required for FDA approval for changes made even by the manufacturer, public disclosure of changes prior to the changes being adopted means that patients will be put at increased risk from bad faith attempts to modify devices during the period required to develop and obtain approval for the change. This can be as long as 1-2 years, much longer than the usual time required to issue a patch for conventional network software.

Third, the ability to reprogram these devices after implant is very limited – a typical older implantable pacemaker has only about 100K of RAM, for example, and most of that is needed to hold the data needed for normal operation of the pacemaker. There are patients with older implanted devices for whom there may be no way to change the device without surgically replacing it. These patients will be placed at risk from public disclosure for the remaining lifetime of their implanted devices, which may be as much as 15 years.

We thank you for considering IPO's comments and would welcome any further dialogue or opportunity to provide additional information to assist your efforts on this important issue.

Sincerely,

Herbert C. Wamsley
Executive Director