This is a Word document that allows users to type into the spaces below. The comment may be single-spaced, but should be in at least 12-point type. The italicized instructions on this template may be deleted.

UNITED STATES COPYRIGHT OFFICE

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

Comments of ACT | The App Association on Proposed Class 9: Literary Works-Medical Device Data

ITEM A. COMMENTER INFORMATION

ACT | The App Association
Morgan Reed
President
1401 K Street, NW
Suite 501
Washington, District of Columbia 20005
(202) 331-2130
mreed@actonline.org

ACT | The App Association, representing more than 5,000 app companies and software firms that create and license digital content, submits the following comments to the United States Copyright Office ("Copyright Office') in response to its Notice of Proposed Rulemaking ("NPR") concerning possible temporary exemptions to the Digital Millennium Copyright Act's ("DMCA") prohibition against the circumvention of technological measures that control access to copyrighted works. The App Association is widely recognized as the foremost authority on the $1.7 trillion app ecosystem and its intersection with governmental interests. As the only organization dedicated to the needs of small business app developers and tech innovators around the world, the App Association advocates for an environment that inspires and rewards innovation while providing the resources to help our members leverage their intellectual assets to raise capital, create jobs, and support innovation.

ITEM B. PROPOSED CLASS ADDRESSED

Proposed Class 9: Literary Works- Medical Device Data

ITEM C. OVERVIEW

ACT | The App Association opposes the proposed class 9 exemption that modifies the current exemption for medical device data by expanding the means of circumvention beyond passive monitoring of wireless transmissions, eliminating the limitation to devices that are "wholly or partially implanted," permitting third parties to perform the circumvention, and removing language requiring consideration of other applicable laws. Petitioners have failed to establish that they are or are likely to be harmed in their ability to make non-infringing uses of a class of copyrighted works because of the prohibition on circumvention without the proposed changes to the current exemption covering access to patient data on networked medical devices. If adopted, the proposed exemption on access to patient data will negatively impact the thriving marketplace of innovation for mobile health products and services. In addition, the proposed exemption would negate federal and international regulations and guidance to ensure the safety and efficacy of medical devices and laws to protect patient data privacy. App developers use technological protection measures to protect their intellectual assets but also to comply with state and federal privacy laws. It is impossible to isolate the copyright issues from the laws, regulatory regimes, and voluntary industry initiatives intended to protect patients that makers of medical devices and software must adhere to. The Copyright Office should not recommend adoption of this proposed exemption without first consulting the relevant agencies and stakeholders involved in deploying medical devices.

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

ACT | The App Association developed a program dedicated to its members engaged in the delivery of mobile health products and services. The Connected Health Initiative or "CHI" (www.connectedhi.com) is a coalition of industry stakeholders and partners leading efforts to harness the power of technology to improve patient engagement and health outcomes, with members that include healthcare providers, insurers, digital health vendors, and connected health technologies. CHI represents a broad consensus of stakeholders across the healthcare and technology sectors whose mission is to support the responsible and secure use of connected health innovations throughout the continuum of care to improve patients' and consumers' experience and health outcomes. CHI commits to advancing an interoperable healthcare continuum that enables the bidirectional flow of necessary health data between provider and patient, as well as between other important stakeholders who have a role in improving care coordination and decision-making.

Data and clinical evidence from a variety of use cases continue to demonstrate how the connected health technologies available today—whether called "telehealth," "mHealth," "store and forward," "remote patient monitoring," or other similar terms—improve patient care, prevent hospitalizations, reduce complications, and improve patient engagement, particularly for the chronically ill. Connected health tools, including wireless health products, mobile medical device data systems, telemonitoring-converged medical devices, and cloud-based patient portals are able to fundamentally improve and transform American healthcare. By securely enabling the exchange of health information and incorporating patient-generated health data (PGHD) into the continuum of care, these tools can render meaningful and actionable outcomes.

Innovative app developers rely on technological protection measures like authentication and encryption to allow legitimate uses of medical devices, ensure the product works as intended, and protect user privacy. Petitioner's proposal poses a serious threat to developers of connected health devices to comply with their legal obligations, protect patients, and be successful in the marketplace.

1. The Petitioner for Proposed Class 9 has failed to meet the standard required to grant an exemption.

In the NPR, the Copyright Office sets the standard for granting a temporary exemption from the prohibition on circumvention dictated by the DMCA. The DMCA allows exemptions when "persons who are users of a copyrighted work are, or are likely to be in the succeeding 3 year period, adversely affected by the prohibition… in their ability to make non-infringing uses under [title 17] of a particular class of copyrighted works." The proponents for the *Petition for a New Exemption and Round 1 Comments* fail to provide evidence to support the claim that users of any networked medical device need unrestricted ability to circumvent technical protection measures (TPMs) protecting software to access patient data or to employ outside assistance to do so.

Petitioner has not presented distinct and measurable evidence that the circumvention prohibition is adversely affecting their ability to make non-infringing uses of medical device data or that it will likely have an adverse impact in the next three years. In fact, the opposite is the case. The proposed exemptions would remove all restrictions on circumvention of medical devices, yet the petitioner focuses almost exclusively on the Continuous Positive Airway Pressure or "CPAP" machine. And the petitioner admits to using "free open-source software to circumvent TPMs on CPAP machine SD cards—rather than passively monitor wireless transmissions emitted from CPAP machines." The petitioner describes how CPAP users can get their personal data using "SleepyHead" or "OSCAR" programs. Aside from the fact that these programs appear to violate the DMCA and go beyond the existing exemption, the problem articulated is not an inability to get the data but rather "a substantial shortage of sleep apnea specialists across the United States" who can provide patients with appropriate treatment.

Medical device users have other legal options to obtain their health data and to file complaints about the performance of a device. The Department of Health and Human Services ("HHS") issued a final rule implementing a prohibition on information blocking included in the Cures Act. Further, the Federal Drug Administration ("FDA") has an online complaint form on its website where medical device users can submit information about device functionality. It does not appear from the Petitioner's comments that these options have been utilized to address concerns about the consistency, reliability, or readability of data from CPAP machines or to receive readable copies of personal data. Therefore, the prohibition on circumvention, beyond the current exemption, is arguably adversely impacting the ability of the Petitioner to make non-infringing uses of medical device software and the proposed new exemption should be denied.

2. The Proposed Class 9 exemption will undermine laws, regulations and voluntary stakeholder standards that ensure medical devices are safe, effective, and protect patients' medical records.

Petitioner's proposal to allow third parties to facilitate the circumvention of TPMs on software operating medical devices will cause developers of connected health devices to be in violation of their legal obligations to protect consumer safety and privacy. It is imperative that the Copyright Office understand the complex legal, regulatory, and voluntary standards regimes involved in the development of medical devices for use by patients. Contrary to petitioner's argument otherwise, these laws are not irrelevant to the process but are critical safety measures resulting from extensive work with stakeholders and policymakers.

The use of digital rights management tools (DRM) or TPMs is critical to protection against unauthorized access to the copyright protected software but also against attempts to steal personal information. In fact, digital products and services developed for every industry must comply with federal, state, and international privacy laws to protect consumer privacy. The Children's Online Privacy Protection Act (COPPA), the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act, the California Consumer Privacy Act (CCPA), and the EU's General Data Protection Regulation (GDPR) are just some of the laws requiring tech developers to use technical means, including encryption, to protect consumer information. This technical protection, whether used for DRM or privacy, has the same underpinning. It is impossible to isolate the issue of whether to expand DMCA exemptions to only the copyright concerns. The vast personal information accessed through the mobile apps on smartphones and connected devices must be protected according to these laws.

Allowing patients access to their medical records is important. HHS and the FDA have prioritized initiatives to make it easier and safer for patients to obtain their data. The Office of the National Coordinator ("ONC") for Health Information Technology, under HHS, announced rules on information blocking in the Cures Act Final Rule. Information blocking—a practice by a health IT developer, information network, or provider that is likely to interfere with access, exchange, or use of electronic health information—is prohibited, unless exempted for reasonable and necessary activities. Exemptions to information include activities necessary to prevent harm to patients and to protect patient privacy. Complaints of information blocking can be submitted through the ONC's online form, providing patients an option to obtain their medical data.

The FDA's Center for Devices and Radiological Health (CDRH) is responsible for regulating firms thta manufacture, repackage, relabel, and/or import medical devices sold in the United States. It is the goal of the FDA to ensure that medical devices used in the United States are safe and effective. Advances in technology have made software integral to medical devices, and it can be classified as a medical device itself. Medical devices are classified according to the risk they pose for illness or injury. Class III devices, which the Petitioner references in comments, create a significant risk to patient health if they do not operate properly. These devices must go through an extensive premarket approval process and be subject to the quality system ("QS") regulations and device reporting requirements in the event the device may have caused or contributed to a death or serious injury. And, in 2016, the FDA issued post-market guidance for managing cybersecurity vulnerabilities for medical devices. It encouraged developers of medical devices to address cybersecurity threats throughout the product lifecycle because the exploitation of vulnerabilities may represent a risk to the health of users. The FDA does not have a process to review third-party modifications of devices to ensure they operate safely. It does, however, have an online portal to report product quality concerns, such as unreliable and incomplete data produced by different CPAP manufacturers.

Allowing third parties to perform circumvention on behalf of a patient in order to obtain medical device data, beyond the passive monitoring of wireless transmissions permitted under the current exemption, will result in devices being out of compliance with FDA regulations, compromise the performance of the device, and put users' health in jeopardy. The App Association strongly opposes this proposed change to the exemption for medical device data.

3. The Proposed Class 9 is overly broad and would undermine innovation in the marketplace for mobile app health products and services.

In the NPR, the Copyright Office states that in evaluating the evidence presented with respect to a proposed exemption, it must consider "the effect of circumvention of technological measures on the market for or value of copyrighted works;…" Granting the proposed new exemption for medical device data will negatively impact the ability of app developers to successfully compete in the mobile health marketplace and protect users from risk of malfunctioning devices and data breaches.

Allowing any manner of circumvention of TPMs on any medical device, whether "wholly or partially" implanted, would eliminate critical protections for developers of connected health devices to improve product performance and combat piracy and cyberattacks that harm developers and consumers alike. While the proponent may have good intentions, the reality is that an unrestricted exemption from the prohibition on circumvention of TPMs controlling access to medical device data exposes the entire mobile health marketplace to piracy. For App Association members, TPMs and legal protections of the DMCA not only secure the economic viability of the business, but they also help them to secure software so that customers, or patients, are safer. Innovative app developers rely on firmware TPMs like authentication and encryption to allow legitimate uses of works and mitigate serious threats to user privacy. For example, Mimir Health makes cloud-based analytic software for healthcare executives and clinicians. The company's products combine disparate healthcare data into one place, eliminating time wasted on data consolidation and preparing reports by hand. Using strong TPMs is essential to protecting patient data and maintaining client trust.

TPMs protect layers of software in devices. Licensed software is part of most products with digital content embedded in them. The system of licensed software is a crucial component to the investment and distribution in existing products and future innovations. The benefits to consumers—and patients—across a wide variety of products and services at every price point cannot be understated. Exemptions that allow circumvention of TPMs protecting embedded device software compromise the protections afforded to other licensed software, putting consumers and their personal information at risk when products malfunction. It also allows software competitors access to product codes which is a disincentive to innovation. The proposed new exemption would open the door to access the proprietary codes of all medical and health monitoring devices created and supported by mobile app developers, disincentivizing innovation and putting consumers at risk.