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 12: Computer Programs- Repair

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 drive innovation.

ITEM B. PROPOSED CLASS ADDRESSED

Class 12: Computer Programs- Repair

ITEM C. OVERVIEW

ACT | The App Association opposes the proposed new exemptions to allow circumvention of technological protection measures controlling access to all embedded software in medical devices, video game consoles, devices or machines for purposes of repair, diagnosis, or modification. The intended "uses" of embedded software in devices and machines manufactured and sold in nearly every industry do not qualify for a blanket determination of "fair use." And, the petitions fail to prove actual harm to non-infringing uses, which is the standard in the DMCA, not "But I want to do something with my device that the manufacturer does not allow." The protections in the DMCA enable creators and innovators to develop and distribute digital products and services at a range of price points that benefit consumers. Petitioners' comments do not address the availability of open-source software to build custom devices, damage warranties, and certified repair options available in the marketplace to address their concerns. However, the potential damage to all software markets—mobile apps, enterprise software, and firmware—is significant if these exemptions are approved. These issues can't be viewed as simply copyright issues. The implications for software developers and consumers are not theoretical. Developers have legal obligations under multiple laws and regulations to develop and maintain safe and effective devices that protect consumer privacy. The App Association encourages the Copyright Office to seek input from the relevant agencies and stakeholders before adopting any exemptions for embedded software on devices.

ITEM D. TECHNOLOGICAL PROTECTION MEASURE(S) AND METHOD(S) OF CIRCUMVENTION

The Petitioners seek abstract exemptions covering circumvention of access controls on embedded software on game consoles, medical devices, and, in the EFF and iFixit petitions, virtually all devices and machines.

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

1. Summit Imaging and Transtate Equipment Company Petition

ACT | The App Association opposes the proposed class 12 exemption to permit circumvention of technical protection measures (TPMs) on software that control the functioning of medical devices for purposes of diagnosis, repair, or modification by or on behalf of the device owner. If adopted, the proposed exemption will negatively impact the thriving marketplace of innovative 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.

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 (CHI) is a coalition of industry stakeholders and partners leading efforts to harness the power of technology to improve patient engagement and health outcomes. CHI members include providers, payers, 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 ability to comply with their legal obligations, protect patients, and be successful in the marketplace.

A. The Proposed Class 12 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 mobile apps on smartphones and connected devices must be protected according to these laws.

The FDA's Center for Devices and Radiological Health (CDRH) is responsible for regulating firms that 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 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. In 2016, the FDA issued post-market guidance for the 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.

B. The Proposed Class 12 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 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. An unrestricted exemption from the prohibition on circumvention of TPMs controlling access to medical device software 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 their businesses, but they also help secure software so that consumers, 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 overstated. 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.

2. **Public Knowledge, iFixit, and EFF Petitions**

The App Association opposes the proposed class 12 exemption to permit circumvention of TPMs to access embedded computer software on any device for the purpose of diagnosis, repair, modification, or replacement of damaged hardware. The proposed class is overbroad and will have an adverse impact on the mobile app industry as well as consumers.

Section 1201 of the DMCA intentionally set a high bar for exemptions to circumvention that allow access to copyrighted works. The rulemaking process is specifically designed to give the law flexibility to address actual harms to the lawful uses of copyrighted works based on evidence presented by users. The hurdle is proof of harm. Lowering the bar for temporary exemptions will recalibrate the balance intended in the DMCA.

Broad exemptions that allow circumvention for device repair will undermine the important incentives in the DMCA for creators and jeopardize the safety and privacy of consumers. App Association members, inventors and entrepreneurs themselves, understand and appreciate the desire to reconfigure the software on a device, create new functionalities, and repair hardware. However, the DMCA exemptions and those adopted by the Copyright Office in these rulemaking proceedings must maintain the balance of interests in protecting copyrighted works while allowing users to access and use those works. Before considering the further expansion of exemptions to cover broad categories of works, it is important to know that developers, inventors, tinkerers, and repair services who want to build their own solutions or fix their own devices have plenty of options available to them. Both closed and open-source systems are flourishing, giving innovators and consumes the ability to choose the ecosystem that works best for them. For example, Apple Repair is a private industry solution that provides customers with flexible options and at the same time protects the content and the integrity of the software. Apple has set up a certification program for independent repair shops where providers can get trained and certified. The network of Apple Authorized Service Providers is nationwide, including in all Best Buy stores. Apple Repair is just one example of many where private industry is providing users with the tools to use and enjoy their products safely.

TPMs protect layers of licensed 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 across a wide variety of products and services at every price point cannot be overstated. Exemptions that allow the offering of third-party assistance or tools to circumvent 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. Fortunately, there are alternative options to address many of the concerns expressed regarding access to software. Notices to consumers about restrictions and allowable uses along with offering certified third-party repair services can protect consumers and software developers. App Association members and those of other content and tech industries rely on licensed software to continue to offer low-cost, consumer friendly products across a growing range of business models.

Innovative app developers rely on firmware TPMs like authentication and encryption to allow legitimate uses of works and mitigate serious threats to user privacy. The use of DRM or TPMs is critical to protection against unauthorized access to a copyrighted work 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 to 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. By law, the vast personal information accessed through mobile apps on smart devices and appliances must be protected. The use of TPMs is necessary to maintain the integrity of software, protect end-user data collected by consumer products with embedded software from nefarious actors, and uphold the obligation to protect consumers' privacy rights.