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 5: Computer Programs- Repair

ITEM A. COMMENTER INFORMATION

ACT | The App Association
Morgan Reed, President
Brian Scarpelli, Senior Global Policy Counsel
Priya Nair, Senior Intellectual Property Policy Counsel
1401 K Street, NW
Suite 501
Washington, District of Columbia 20005
(202) 331-2130
mreed@actonline.org

ACT | The App Association (the App Association) is a policy trade association for the small business technology developer community. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. App developers like our members also play a critical role in developing entertainment products such as streaming video platforms, video games, and other content portals that rely on intellectual property (IP) protections. The value of the ecosystem the App Association represents—which we call the app ecosystem—is approximately $1.8 trillion and is responsible for 6.1 million American jobs, while serving as a key driver of the $8 trillion internet of things (IoT) revolution. App Association members rely on strong cybersecurity protections, patenting, and copyright to protect their valuable IP. The Digital Millennium Copyright Act (DMCA) is a foundation of many of those protections.

ITEM B. PROPOSED CLASS ADDRESSED

Proposed Class 5: Computer Programs - Repair

ITEM C. OVERVIEW

The App Association opposes the proposed new exemption to expand the repair exemption for consumer electronic devices to include commercial industrial equipment such as automated

building management systems and industrial equipment (i.e., soft serve ice cream machines and other industrial kitchen equipment) for purposes of diagnosis, repair, modification, or replacement of damaged hardware. We opposed the proposed the overbroad proposed exemption for damaged consumer electronic device in 2021; we oppose its attempted renewal; and we oppose its expansion through this petition.

The intended "uses" of embedded software in consumer electronic devices manufactured and sold in nearly every industry do not qualify for a blanket determination of "fair use." And, this petition fails to provide any evidence of 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 this exemption is 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 to broaden the repair exemption for consumer electronic devices to include commercial industrial equipment such as automated building management systems and industrial equipment. This proposed exemption seeks to expand on a previous exemption to the prohibition against circumvention of technical protection measures (TPMs) for computer programs that control devices designed primarily for use by consumers for diagnosis, maintenance, or repair of the device or system. Such TPMs include encryption software that allows copyright rights holders to control the ability for third parties to access and copy protected works.

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

1. Public Knowledge, iFixit Petitions

The App Association opposes the proposed class 5 exemption to permit circumvention of TPMs to access embedded computer software for the purpose of diagnosis, repair, modification, or replacement of commercial industrial equipment. The proposed class is overbroad and will have an adverse impact on the mobile app industry as well as consumers. For small businesses, like App Association members, mandates to allow open access to otherwise protected software involves legalizing a "market for exceptions" that can lead to increased cyberattacks. This type of security risk is especially prominent when the software in question deals with encryption or other vital security tools, including TPMs.

The circumvention prohibitions and exemptions under Section 1201 of the DMCA have proven to be effective and flexible tools that enable continued innovation in the tech sector and promote consumer choice. The DMCA has only two prohibitions to prevent unauthorized access to digital content – the act of circumvention of TPMs and the distribution of tools and technologies used for circumvention of TPMs. Congress included 10 key exemptions that allow the circumvention or breaking of digital locks on copyrighted works and the creation of tools to allow these activities. These safety valves—intended to balance copyright rights with the public interest in accessing and using copyright protected content—actually work. Developers rely on these exemptions to innovate, which in turn provides consumers with access to a wide range of products and services in a variety of business models.

The DMCA exempts security testing, encryption research, and reverse engineering activities from the prohibition on circumvention within certain parameters. These activities are important and necessary parts of developing software products and services that entertain and meet the needs of consumers. For example, there is a considerable record of published results from security testing on automotive security, medical devices, voting systems, and consumer devices. Likewise, reverse engineering allows developers to create new interoperable and competing products and services. And encryption research is critical to improving technology to protect most internet traffic—everything from commercial transactions to social interactions. Our members like to say, "Just tell us the rules so we can build our business." The exemptions in the DMCA provide clear guidelines for app developers as they create and bring their products to market. This is why the DMCA intentionally sets a high bar for further exemptions to Section 1201 prohibitions 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 has developed four streams of options for consumers. Malfunctioning technology can be brought to an Apple Store or mailed to Apple, customers can use an Authorized Service Provider like Best Buy, they can find an Independent Repair Provider in the network, or they can utilize Apple's Self Service Repair. 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.

Apple Repair is just one example of many where private industry is providing users with the tools to use and enjoy their products safely. These voluntary actions from numerous companies are driven by market demand and provide the ability for end users to repair products while protecting intellectual property and end user safety

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 Digital Rights Management (DRM) or TPMs is not only 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.