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 4: Computer Programs – Generative AI Research

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 4: Computer Programs – Generative AI Research

ITEM C. OVERVIEW

The App Association opposes the proposed new exemption to facilitate essential security research on generative artificial intelligence (GAI) models and systems, specifically concerning biases embedded within them.

The intended "uses" of embedded software in any technology deployed in nearly every industry do not qualify for a blanket determination of "fair use." And, this petition fails to provide any evidence that remedies of law or regulation are not sufficient to prevent actual harm to non-infringing uses, which is the standard in the DMCA. Petitioner's comments do not address the potential damage to all software markets—mobile apps, enterprise software, and firmware— by imposing a broad exemption that allows anyone to circumvent GAI models for "essential security research," a factor that is not clearly defined. While questions of security, privacy, and IP persist in the deployment and use of GAI models, the widening of Section 1201 exemptions is not the solution. Stakeholders, including the App Association, should turn to policymakers and regulators to comprehensively define the contours around AI, including for essential security research related to race, gender, ethnicity, and other sensitive factors. The App Association encourages the United States Copyright Office ("USCO" or the "Office") to seek further input and evidence from the relevant agencies and stakeholders before adopting any exemptions on GAI models.

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

The Petitioner proposes a new exemption to facilitate essential security research on GAI models and systems, specifically concerning biases embedded within them. This proposed exemption seeks to bypass legislative and regulatory efforts that are already underway to create more transparency in the deployment of GAI models, while defending the rights of their providers to protect IP and proprietary works. Technological protection measures (TPMs) for this technology often include encryption software that allow copyright holders to control the ability for third parties to access and copy protected works.

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

1. Jonathan Weiss Petition

The App Association opposes a new class 4 exemption to facilitate essential security research on GAI models and systems, specifically concerning biases embedded within them. The proposed class is overbroad and will have an adverse effect on the software developer industry writ large as well as consumers using GAI models. 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 their 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 already 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 of TPMs 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 require emerging technology platforms, which they both provide and use, to take reasonable steps to protect the privacy, security, and IP of their platform users and other external IP rights holders. However, the DMCA exemptions and those adopted by the Office in these rulemaking proceedings must maintain the balance of interests in protecting copyrighted works while allowing users to access and use those works.

For software developers, including App Association members, public facing GAI models are an invaluable component of creative and innovative processes by reducing wasted resources (i.e., cost and time), streamlining repeatable tasks, and optimizing solutions. For software coders, platforms like Microsoft’s GitHub Copilot have turned hours of coding into minutes, a competitive edge that startups and small businesses cannot afford to lose. In the same vein, there are invoked fears around how GAI models can harm user privacy, security, and IP protections. App Association members operate with minimal resources and are most acutely harmed by unpredictable copyright outcomes related to liability. Until the USCO establishes a report on their recent study of the copyright law and policy issues raised by AI systems, we urge the agency to reject any argument to implement exemptions for AI systems. Adopted exemptions to Section 1201 prohibitions should not be driven by edge use cases or hypotheticals that exemplify possible uses and capabilities of AI outside what we presently understand.

The App Association provides a strong voice on shaping rules for complex and evolving AI and brings the small business voice to the table. We propose principles that define a successful policy approach that targets the benefits, risks, and challenges presented by evolving AI tools in use cases for software development verticals. These principles include supporting research and transparency in the development of AI, modernizing privacy and security frameworks to the capabilities of AI, and addressing AI bias. We acknowledge that the potential for harmful bias (whether racial, political, geographic, etc.), as well as errors, will remain one of the more pressing issues with AI systems that utilize machine learning techniques. Stakeholders throughout the chain, including AI deployers, developers, and consumers, should develop and measure adherence to diversity, equity, and inclusion best practices to identify, address, and mitigate the risks of harmful bias that may affect marginalized and underrepresented groups. Regulatory agencies should examine data provenance and bias issues present in the development and uses of AI solutions to ensure that bias in datasets does not result in harm to users or consumers of products or services involving AI, including through unlawful discrimination. These considerations provide justification for a comprehensive policy framework, not for broad exemptions that weaken the enforcement of Section 1201 of DMCA.

Before considering the further expansion of exemptions to cover broad categories of works, it is important to understand that market pressures drive voluntary actions from numerous companies to allow end users to bypass Digital Rights Management (DRMs) and TPMs for narrow purposes while protecting intellectual property and end user safety. It is important to support voluntary actions by GAI platform developers rather than subjecting them to overbroad exemptions to Section 1201 that disincentivizes the creation of these types of advanced technologies.

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 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.

Innovation relies 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 stored within a GAI model. In fact, GAI models 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 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.