ACT

The App Association

March 3, 2016

The Honorable Maria A. Pallante
Register of Copyrights
U.S. Copyright Office
101 Independence Avenue, SE
Washington, DC 20559-6000

RE: Comments of ACT | The App Association in Response to the U.S. Copyright Office's Notice of Inquiry, *Section 1201 Study: Notice and Request for Public Comment*, 80 FR 81369 (Dec. 29, 2015)

Dear Ms. Pallante:

ACT | The App Association, representing over 5,000 app companies and software firms creating and licensing digital content, submits these comments in response to the Copyright Office's Notice of Inquiry regarding the operation of section 1201 of Title 17, including the triennial rulemaking process established under the Digital Millennium Copyright Act[1] ("DMCA").[2] ACT is widely recognized as the foremost authority on the $120 billion mobile app economy and its intersection with public policy. As the only organization focused on the interests of small business app developer entrepreneurs around the world, ACT advocates for policies that inspire and reward innovation and provides resources to help its members leverage their intellectual assets to raise capital, create jobs, and continue innovating.

ACT's views on the effectiveness of Section 1201 are informed by several core principles:

- ***Copyright Laws Should Encourage Creativity and Innovation while Protecting Consumer Interests:*** The United States' copyright laws were created to stimulate creativity and innovation for the general public good. In any review of the law, its impact, and effectiveness, it is important that the Constitutional balance and Congressional intent underlying the copyright law remains the lodestar, ensuring that the exclusive rights of copyright owners remain meaningful and effective, and preserving the properly-scoped application of limitations on those rights, including fair use.

- ***Copyright Laws Should Permit for the Securing of Digital Content:*** Software application developers continue to face significant harm due to piracy. The tools to address these threats provided by the DMCA, including prohibitions against the circumvention of technological

[1] Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).

[2] *Section 1201 Study: Notice and Request for Public Comment*, 80 FR 81369 (Dec. 29, 2015) ("NOI").

protection measures (TPMs), should be enabled, and not discouraged. The DMCA's anti-circumvention provisions have fueled the availability of new distribution models that have provided new choices to consumers and allowed rights holders to reasonably protect their creative works.

- ***Changes to Copyright Laws Should Respond to Proven Harms:*** Calls for sweeping changes to U.S. copyright law – and particularly the DMCA – based on theoretical or anecdotal harms and speculative impacts should be rejected.   ACT urges the United States Copyright Office (USCO) to ensure its report is data-driven and that any recommendations for reform are based on proven – not theoretical – harms.

- ***Sector-Specific Issues should be Addressed by Relevant Federal Actors, Not Through Altering the Copyright Laws:*** In addressing concerns beyond core copyright issues, care should be taken to ensure that proposals for changes to section 1201 or the 1201 process do not become a vehicle to effect policy considerations more appropriately addressed through other laws or by other agencies.

- ***Changes to U.S. Copyright Law and Global Impacts:*** Policymakers examining changes to U.S. copyright law should always consider the impact changes made to copyright law in the context of a digital economy may have in creating precedent outside of the United States.

I. ACT | The App Association's views regarding the role and effectiveness of the prohibition on circumvention of technological measures in Section 1201(a)[3]

As detailed in ACT's latest *State of the Mobile App Economy* report,[4] the app industry has existed for less than a decade and has experienced exponential growth alongside the rise of smartphones. It now represents a $120 billion ecosystem which is led by U.S. companies, the vast majority of which are startups or small businesses. The explosion of business-to-consumer and business-to-business mobile apps being deployed by non-traditional software companies is dramatically changing the independent software vendor economy, specifically with regard to exposure to digital risks and vulnerabilities. These deployments include a variety of content delivery options, security and monitoring services, tech support services, payment processing services, patents, licensing agreements, and diverse revenue models. Copyright protections should contemplate dynamic industries like the mobile app economy, and are a crucial underpinning to ACT's thousands of software development member companies' business models, such as:

- Health devices with embedded software that are relied upon for related decisions, ranging from lifestyle changes to medical treatments.
- Automotive products with embedded software that drivers rely on to protect their safety on American roadways.
- Software tools used by countless Americans to handle financial transactions.
- Consumer and home-oriented products enabled by embedded software apps that are relied upon for alertness and safety, as well as convenience and entertainment.

Piracy presents a major threat to the success of ACT members and the billions of consumers who rely on digital products and services. Piracy, whether originating within the U.S. or abroad, threatens not only the creators of digital content by undermining their ability to innovate, invest, and hire. It also threatens the end-users' confidence in products and services as there is potential for consumers to be victimized by illegal sellers who pose as legitimate content owners and sellers. Counterfeiting software apps can lead to customer data loss, interruption of service, revenue loss, and reputational damage. Further, with the rise of enterprise mobile app development, apps are being used as a means to attack mobile users of an entire enterprise. While the criminal penalties for these activities (*e.g.*, attacking a bank's clients through a counterfeit version of their app) are likely more of a deterrent than the copyright laws being violated when the counterfeit app is created, these criminal acts all begin with first misappropriating application logic and application media content (brands, etc.). These threats have caused significant damage, and continue to pose substantial hazards, to app development companies that service every sector of the economy for countless end-users. It is absolutely essential for copyright owners to be able to utilize encryption and other forms of access controls to combat these threats.

[3] NOI at 81373.

[4] ACT's annually-released *State of the Mobile App Economy* provides further information on this growing industry that continues to grow, creating jobs and revolutionizing how consumers work, play, and manage their health. *See* http://actonline.org/2016/01/04/act-the-app-association-releases-latest-app-industry-report/.

For example, ACT member BusyBee Studios' children's app Zoo Train[5] was featured in the GooglePlay app store for sale at $0.99. This app uses colorful animal shapes and animations in providing educational puzzles and spelling lessons for young children. During a search for the product, the developers found another app in the GooglePlay store using the same name and artwork, but from a different publisher. This pirated app was free in the GooglePlay store, was displayed as a result of a search query for "Zoo Train," and – unlike the true Zoo Train app – displayed advertisements to earn bogus revenue as well as gained permission to control a user's device in order to access phone dialer information, the address book, and the network stack to install itself to run in the phone's operating system background to collect this information (in other words, a malware "stub" that sits inactive but can be activated with a command).

Other innovative mobile app innovators rely on TPMs, such as authentication and encryption to allow legitimate uses of works and to mitigate serious piracy threats. For example:

- Mimir Health,[6] which 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.

- DrinkMate,[7] producer of the smallest breathalyzer in the world that plugs into a smartphone. Once plugged into a smartphone and activated via its software app, a user can blow into the device and get an immediate reading of blood alcohol content. DrinkMate's goal is to promote safe and responsible drinking habits and personal/public safety.

- PreEmptive Solutions,[8] which provides application protection solutions, and works directly with many thousands of software development organizations to help them manage these specific risks. Leveraging PreEmptive's application analytics and protection solutions, development organizations materially improve application quality, user satisfaction, and development ROI across today's distributed and increasingly heterogeneous computing architectures.

The app industry effectively did not exist when the DMCA became law in 1998 after a comprehensive negotiation between policymakers, copyright interests, tech firms, network operators, and nonprofits. The DMCA, and the Copyright Act itself, was never expected to end unlawful uses of content. No laws, for that matter, can prevent unlawful behavior entirely. While the DMCA has not eliminated digital piracy, it has provided important tools for copyright owners to protect their works online. The DMCA is not without flaws, but it and the Section 1201 process have proven effective and flexible tools to provide for and deal with continued innovation in the tech sector and to promote consumer choice. Further, the courts have reined in attempts to abuse the law and stretch its protections to yield unintended results or consequences.[9]

[5] https://itunes.apple.com/us/app/zoo-train/id407870968?mt=8.

[6] http://www.mimirhealth.com/.

[7] http://www.getdrinkmate.com/.

[8] https://www.preemptive.com/.

[9] *See*, *e.g.*, Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004).

II. ACT | The App Association's views on how Section 1201 and its relation to interests that are outside of core copyright concerns (*e.g.*, "cases where circumvention of access controls protecting computer programs implicates issues of product interoperability or public safety")[10]

Generally, we urge the USCO to very carefully approach instances where Section 1201 addresses issues beyond core copyright concerns and to ensure that its related actions do not supplant the mechanisms and processes in place to address public policy objectives beyond the goals of section 1201 to protect copyrighted works and encourage new mechanisms for their dissemination. To the extent that other public policy concerns are raised or implicated, we urge the Office seek the guidance and expertise of other expert agencies. As it did in the 2015 rulemaking process, the Office can and should take reasonable additional time to shape appropriate exemptions with input from other agencies.

***

[10] NOI at 81373.

ACT | The App Association appreciates the opportunity to submit comments to the USCO to help inform the record and its study regarding the operation of section 1201 of Title 17, including the triennial rulemaking process established under the DMCA to adopt exemptions to the prohibition against circumvention of technological measures that control access to copyrighted works, and looks forward to the opportunity to meet with you and your team to discuss these issues in more depth. Thank you for your consideration.

Sincerely,

Morgan Reed

Morgan Reed
Executive Director
ACT | The App Association