ACT | The App Association

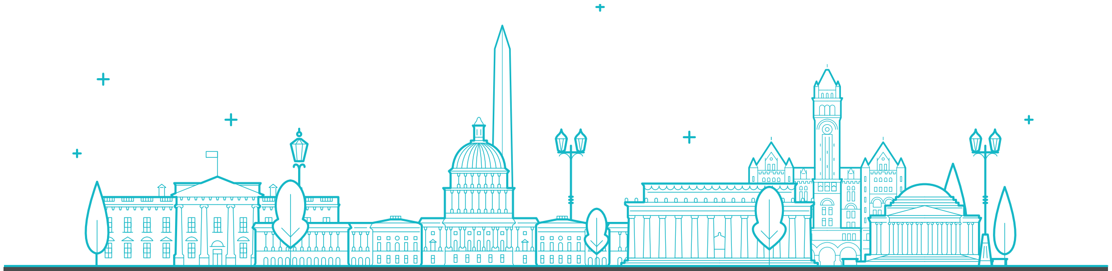
Are Reforms to Section 1201 Needed and Warranted?

Testimony of

Morgan Reed
President
ACT | The App Association

Before the

U.S. Senate Judiciary Committee,
Subcommittee on Intellectual Property



1401 K Street NW Suite 501
Washington, DC 20005

☎ 202.331.2130
www. ACTonline.org

@ACTonline
/ACTonline.org

I. Introduction

We thank the Senate Judiciary Subcommittee on Intellectual Property for holding this hearing on Section 1201 of the Digital Millennium Copyright Act (DMCA). This hearing provides an important opportunity to highlight how, since enactment, the DMCA both protects the interests of creators and rightsholders and enables exponential growth in technological innovation. ACT | The App Association is the voice of small business tech entrepreneurs, and we appreciate the Subcommittee welcoming the views of our members on how best to safeguard content creation and to foster an innovative and safe marketplace for consumers. In short, the DMCA is working for app developers and their customers.

The App Association is a trade group representing about 5,000 small to mid-sized software and connected device companies across the globe. In the United States, our member companies are part of a $1.7 trillion industry, supporting about 5.9 million jobs. If these seem like surprisingly high figures, it could be because there is a tendency to look only at the consumer-facing or the top 100 most-downloaded apps in the Apple App Store or Google Play store when referencing the market for apps. But these are a small fraction of the app economy. Most of our member companies make white label software—that is, they build software and provide services for other companies. If a member company makes an app for another firm, the client's logo usually goes on the app. And the app itself may not be consumer-facing at all—it may be a management program for internal use by a brewery, hospital, or manufacturer. What virtually all of them have in common, though, is that they leverage software platforms to reach their clients and customers and depend on strong copyright protections to protect their valuable businesses.

For our members, the technical protection measures (TPM) and legal protections of the DMCA not only secure the economic viability of the business, they also help them to secure software so that their customers, and ultimately the consumer, are safer. This does not mean, however, that our members only rely on restrictive software licensing approaches. In fact, most, if not all, of our members build software utilizing tools that operate under a wide range of licensing structures, from highly permissive licenses like a Berkeley Software Distribution, or BSD, license to the most restrictive per-seat license arrangements. The reality of the software licensing world is that no one license fits every need; having clear rules and legal enforcement mechanisms helps at every license level.

For this hearing, three things stand out:

- **Strong protections against circumvention are necessary because even "free" apps are commonly stolen.** This is important because we often see the debate about the DMCA framed as a referendum on the pricing of content. As I will discuss below, the age of free, ad-supported apps has seen a rise in the piracy of app content, where a stolen version of an app is dropped onto a separate ad network that pays the copyright thief, instead of the original content owner or creator of the original app. Ad industry groups like the Trustworthy Accountability Group (TAG) and others are working to fight click fraud and piracy, but the fact that free isn't cheap enough to stop thieves is an important consideration.

- **TPMs are important for safety and national security.** During the COVID-19 pandemic, every American has moved many of their activities online, making data protection ever more important. Releasing public tools that break encryption puts healthcare, school, and financial information at greater risk. The technical layer that provides digital rights management (DRM) for software, music, and movies is roughly the same. In simplest terms, encryption is math, and tools designed for one kind of decryption are well situated to be used for less honest purposes.

- **The current triennial review process works.** Although every single one of the witnesses here today can list off an example of a triennial review decision they didn't like, the three-year window gives all parties a chance to voice concerns. Accordingly, we do not recommend that Congress amend the statute to require the Library of Congress to conduct these reviews more or less often. Going to a 10-year review or a one-year review would not result in better decisions, just less thought and flexibility.

II. DMCA Allows App Developers to Protect Their Products and Consumers

By enacting the DMCA, Congress sought to promote a robust digital marketplace of products and services. In order to do that, the DMCA gave creators and innovators the right to control access to their works with digital locks to encourage online distribution that would in turn benefit the general public. The DMCA also recognized the reality that there would be honest and reasonable tension between multiple stakeholders and made allowances for technology and consumer behavior changing over time. The App Association believes the law largely accomplished this balancing act and continues to provide app developers with the critically important ability to protect their software from unlawful access. The exponential growth in the app ecosystem, and the wide range of businesses it supports, would not be possible without the protections and incentives in the DMCA.

Like many other industries, the app industry experiences significant loss of revenue each year from piracy and counterfeits. Piracy presents a major threat to the success of App Association members and the billions of consumers who rely on digital products and services. Piracy—whether originating within the United States or abroad—threatens the creators of digital content by undermining their ability to innovate, invest, and hire. Piracy also threatens end-user confidence because it creates the potential for consumers to be victims of illegal sellers who pose as legitimate content owners and sellers. Counterfeit 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, hijacked apps are used to attack mobile users in the enterprise context. While the criminal penalties for these activities (e.g., attacking a bank's clients through a counterfeit version of their app) are likely a greater deterrent than the consequences for the violation of copyright laws, these criminal acts all begin with misappropriating application logic and application media content (brands, etc.). Appropriating intellectual property is often a necessary predicate to carrying out these kinds of cyberattacks, which are damaging to app developers and consumers alike. It is essential that copyright owners utilize encryption and other forms of access controls permitted by the DMCA to combat these threats.

In one illustrative example, App Association member Busy Bee Studios' children's app Zoo Train sold in the Google Play store for $0.99. This app uses colorful animal shapes and animations in educational puzzles and spelling lessons for young children. During a search for the product, the app's developers found an app in the Google Play store that used the same name and artwork, but provided by a different publisher. This pirated app was free in the Google Play store and displayed as a result of a search query for "Zoo Train," but—unlike the true Zoo Train app—displayed advertisements to earn bogus revenue. Busy Bee Studios lost revenue from paid downloads and advertising. The pirate app also gained permission to control a user's device to access phone dialer information, the address book, and the network stack to install itself to run in the background of the phone's operating system to collect this information. In other words, the fake app implemented a malware stub that sits inactive but uses a command to activate the malware and gather users' personal information.

Other innovative app developers rely on firmware technological protection measures 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.

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 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 cell phones today must be protected by law. The hacked Zoo Train app is a perfect example of the privacy risks of counterfeit apps. The use of

TPMs is crucial to maintaining the integrity of software, protecting end-user data collected by consumer products with embedded software from nefarious actors, and upholding the obligation to protect end-users' privacy rights.

III. App Developers Work with Multiple Licensing Models

The software ecosystem has grown and continues to thrive because of the licensing options available to innovate and develop new products. Most developers find success where multiple licensing models exist simultaneously. Traditional and open source licenses provide the flexible options to meet developer objectives in building their products. Most of our members utilize open source software, and many contribute to open source projects. The reality is that Section 1201 of the DMCA has co-existed comfortably in this world of multiple licensing models and our software development ecosystem benefits from this permissive, multiple license model environment. Our members benefit from this model while also benefitting from protections under DMCA for software that is vital to their business success and protection of their customers.

In fact, some of our members will build a product where the underpinning software is open source but the content they provide, like videos and interactive databases, will be protected by TPMs. This ability to mix and match between the software and additional content is critical and demonstrates the flexibility of the current law.

The developer experience with the range of licensing options proves that a change in law is not necessary for the system to work. From small software development businesses to the world's largest companies like Microsoft, Apple, Google, and Intel, all use and contribute to open source software. It is hard to find a chilling effect from the DMCA when developers always have an open source option.

IV. DMCA Exemptions Allow App Developers and Consumers to Innovate

The DMCA is not without its flaws, but the Section 1201 circumvention prohibition and its exemptions have proven to be effective and flexible tools that enable continued innovation in the tech sector and promote consumer choice. While the DMCA has only two prohibitions to prevent unauthorized access to digital content, 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." Well, the exemptions in the DMCA provide clear guidelines for app developers as they create and bring their products to market. The "chilling effect" on innovation that is often raised in the debate about the DMCA simply has not materialized in the app economy. The obvious success of American software-driven industries—which created millions of jobs and leave analogous sectors in other countries perpetually playing catch-up—is strong evidence that the DMCA protections under current law are working.

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's triennial rulemaking process 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 device have plenty of options available to them. Both closed and open source systems are flourishing, giving innovators and consumers 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 Buys. 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 software in devices. Licensed software is a 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 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. 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. Our 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.

V. DMCA Triennial Rulemaking is Working

The DMCA Section 1201 directs the Librarian of Congress, upon recommendation of the Register of Copyrights following a rulemaking proceeding, to determine whether the prohibition on circumvention has, or is likely to have, an adverse effect on users' ability to make non-infringing uses of particular classes of copyrighted works. Users may petition the Copyright Office for exemptions every three years in the triennial Section 1201 proceeding, and the Librarian may adopt limited temporary exemptions waiving the general prohibition against circumvention for such users for the next three years. This 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. And, after completing seven triennial rulemaking proceedings under Section 1201, it is clear that the DMCA safety valve is working.

The Copyright Office should be commended on its administration of an efficient and thorough review process for all requested exemptions. And in each rulemaking, it has granted several exemptions, 14 of which were adopted in the 2018 proceeding. Also in 2018, the Office introduced a streamlined proceeding that would renew exemptions where there is no meaningful opposition to the exemption. The renewed exemptions include literary works where assistive technologies are needed to make it available to persons with disabilities, "computer programs where jailbreaking" phones, tablets, and wearables allows connection of a device to an alternate wireless network, and for the use of short portions of motion pictures for various education and derivate uses. The App Association applauds the Copyright Office for taking the initiative to improve the efficiency of the rulemaking process for all stakeholders.

Still, whether it is the Copyright Office or Congress, the App Association recommends caution when considering new or expanded exemptions to Section 1201 of the DMCA where the issues go beyond core copyright concerns. To the extent requested exemptions raise issues of privacy, consumer protection, interoperability, and data security, additional input from experts and other relevant agencies is imperative.

VI. Conclusion

The App Association has had the same message on Section 1201 of the DMCA for years. The DMCA is working, and changes to copyright law should be responsive to proven harms. The app ecosystem is an example of successful and sustained innovation built on existing laws. Technological innovation will always outpace legislative and regulatory processes, assuring that hastily crafted or overly prescriptive statutory revisions will quickly be outdated, leading to more confusion and frustration in the marketplace. The App Association urges the Subcommittee to ensure that legislative proposals are responding to proven—not theoretical—harms.

Appendix: App Economy Innovators in Your Districts

Majority

Thom Tillis (NC), Chairman

Company: SentryOne

Founded in 2004 and located in Charlotte, SentryOne focuses on creating the most effective and efficient processes for database performance across a variety of platforms. With just under 200 employees, some of the largest companies in the world trust SentryOne to make sure their databases run quickly.

Lindsey Graham (SC)

Company: SC Codes

Founded in 2016 as a collaboration between the South Carolina Department of Commerce's Office of Innovation and Build Carolina, SC Codes is an educational program and platform that works to connect South Carolinians with free workforce development resources in computer science. With only four employees, SC Codes helps both newcomers and experts alike learn new skills, helping students unlock careers in technology for anyone in the state.

Chuck Grassley (IA)

Company: SwineTech

With 13 employees, Swinetech is located in Cedar Rapids and has created an Internet of Things (IoT) device that helps alleviate the strain that piglet crushing has on the agriculture industry. Founded in 2015, Swinetech created Smartguard, a wearable device that senses when there may be a crushing event and encourages the sow to move through sound and vibration.

John Cornyn (TX)

Company: For All Abilities

Founded in 2018 by a former speech pathologist, For All Abilities acts as a de facto chief accessibility officer through the use of software and the founder's own clinical and business experience. Located in Houston, For All Abilities can help businesses meet mandates for accessibility or provide guidance around reasonable employee accommodations as dictated by the Americans with Disabilities Act (ADA).

Mike Lee (UT)

Company: 1564B

Located in Salt Lake City, 1564B is a one-man management consulting group that provides advice on marketing and content development as it relates to technical markets, like the internet of things (IoT). Founded in 2014, 1564B's clients range from startups and growing companies to global corporations.

Ben Sasse (NE)
Company: Quantified Ag (*purchased by Merck Animal Health in June 2020*)
Founded 2014 in Lincoln, Nebraska, Quantified Ag has created what is essentially "Fitbit for cattle" to monitor the health of livestock that often physically hide illnesses from their caretakers. Through early detection, their technology helps dramatically reduce costs by keeping cattle healthy throughout their life cycle.

Mike Crapo (ID)
Company: TaxAct
Founded in 1998, TaxAct is a leading provider of affordable digital and downloadable tax preparation solutions for individuals, business owners, and tax professionals. Their flagship product promises users the highest degree of accuracy and was designed by their own in-house programmers and tax accountants. All available forms are IRS and state approved, and they introduced a mobile application in 2018.

Marsha Blackburn (TN)
Company: Quiet Spark
Established in 2011 in LaVergne, Tennessee, a wife and husband team founded Quiet Spark after noticing their son's issues with spelling. Their first app was SuperSpeller, an iOS app that makes learning spelling fun for children through learning games and reward features. They have also created other apps that help users keep track of their lives through categories like exercise, reading time, scheduling, homework, and more.

Minority
Chris Coons (DE), Ranking Member
Company: Appreneurial
Founded in 2018 and located in Wilmington, Appreneurial is a software development company that offer a diverse array of services including mobile and web development, cloud architecture, UI/UX and others. Everyone on their small team has been an entrepreneur, giving them a unique perspective.

Patrick Leahy (VT)
Company: Aprexis Health Solutions
Aprexis Health Solutions is cloud-based software that helps patients with personalized services for medication therapy management and includes more than 1,000 participating pharmacies and more than 1 million patients. Founded in 2009, Aprexis works with health plans, pharmacy networks, corporate employers, and providers to deliver improved, patient-centric health outcomes.

Dick Durbin (IL)
Company: Devscale
Founded in 2018, DevScale is a software development shop that creates web and mobile apps, as well as Chrome extensions. Although headquartered in Chicago, Devscale has coders all over the world. They take clients all the way through their creative process; from defining the project through user experience stages and development, to the final rollout.

Sheldon Whitehouse (RI)
Company: Blackburn Labs
Located in Providence, Blackburn Labs provides consulting services across a variety of disciplines such as healthcare, education, data literacy, and real estate software, since 2015. Notably, they created a product for Brigham and Women's Hospital called CardioCompass, which helps limit the amount of office visits for patients with chronic conditions.

Richard Blumenthal (CT)
Company: Pixellet
Located in Stamford, Pixellet is a full-service web and mobile development and design firm with dozens of offered services, including digital marketing and e-commerce. Founded in 2014, Pixellet has served a variety of industries including real estate, health care, financial services, and education, among others.

Mazie Hirono (HI)
Company: Smart Yields
Founded in 2015 and headquartered in Honolulu, Smart Yields is an intelligent agriculture software that helps to connect farmers and agricultural researchers to increase crop yield, revenue, and productivity. With fewer than 10 employees, Smart Yields is committed to helping Hawaii meet their commitment to doubling food production by 2030 and other communities achieve similar goals around the world.

Kamala Harris (CA)
Company: BadVR
Located in Marina Del Rey with nearly 15 employees, BadVR is a company that allows clients to examine and conceptualize data through a virtual reality (VR) headset where you can actually see the data for what it is, not just numbers. Founded in 2017, BadVR already has solutions in marketing, smart cities, and telecommunications.