



September 13, 2017

Sarang V. Damle
General Counsel and Associate Register of Copyrights
United States Copyright Office
101 Independence Ave., S.E.
Washington, D.C. 20559

Re: **Exemptions to Permit Circumvention of Access Controls on Copyrighted Works
[Docket No. 2017-10]**

Commenter Information:

This Comment is submitted on behalf of BSA | The Software Alliance (“BSA”), the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world’s most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries around the world, BSA advocates for public policies that foster technology innovation and drive growth in the digital economy.

Proposed Class:

Computer programs that operate smartphones, smart TVs, tablets, or other all-purpose mobile computing devices, to allow the device to interoperate with or to remove software applications (“jailbreaking”).

Basis of Opposition:

BSA opposes renewal of this exemption:

1. This proposal should be rejected because jailbreaking can undermine the integrity and security of a platform’s operating system in a manner that facilitates copyright infringement and exposes users to heightened risks of privacy violations. Congress intended the DMCA to protect the right of platform developers to choose how to design their systems. A manufacturer of computing devices, such as smartphones

and tablets, may choose to curate a “closed ecosystem” in order to create a reliable, secure platform that avoids malware, unstable software, unsuitable content, or other factors that combine to create a platform that consumers want to use to consume a plethora of copyrighted works, including apps, music, movies and television programs. The proposed exemption undermines these design choices.

2. The proposal should likewise be rejected because alternatives to circumvention exist. Only a limited subset of “all-purpose mobile computing devices” include technological protection measures that limit the installation of third-party software applications. The widespread availability of alternative devices negates any minor adverse impact being caused by the presence of access controls on other devices. See 2012 Recommendation at 8 (“If sufficient alternatives exist to permit the noninfringing use, there is no substantial adverse impact.”).
3. The DMCA’s statutory factors also weigh against renewal of the jailbreaking exemption. 17 U.S.C. § 1201(a)(1)(C)(i) instructs the Register to consider “the availability for use of copyrighted works” broadly and in historical context. In the mobile smartphone market, access controls have increased, rather than decreased, the availability of software applications designed for use on mobile phones. For example, BSA member Apple ignited the app revolution with the launch of the App Store in 2008. Since then, an entire industry has been built around app design and development. In the nine years since its launch, App Store customers have downloaded more than 180 billion apps, generating over \$70 billion for the global developer community.¹ The fourth statutory factor, 17 U.S.C. § 1201(a)(1)(C)(iv), also weighs against granting an exemption because circumvention of access controls on tablet facilitates application piracy,² and the value of operating systems designed to reduce piracy is harmed when that feature is eliminated.³

¹ <https://www.apple.com/newsroom/2017/06/apple-unveils-all-new-app-store/>

² Christopher MacManus, *Pirated iOS App Store Installous Shutters*, CNet.com, Dec. 31, 2012, <http://www.cnet.com/news/pirated-ios-app-store-installous-shutters/> (“For many years, Installous offered complete access to thousands of paid iOS apps for free for anyone with a jailbroken iPhone, iPad, and iPod Touch. Think of it as being able to walk into a fancy department store, steal anything you want, and never get caught.”).

³ Cf. 2012 Recommendation at 49.

