

1150 18th Street, NW
Suite 700
Washington, DC 20036

p.202/872.5500
f.202/872.5501

July 2, 2012

BY EMAIL (1201@loc.gov)

Mr. David Carson

General Counsel

U.S. Copyright Office, Office of the General Counsel

Library of Congress

P.O. Box 70400

Washington, DC 20024-0400

Dear Mr. Carson:

The Business Software Alliance is pleased to respond to the questions posed in your letter of June 21, 2012, as follows:

1. Please provide technical details on how Google's Android operating system restricts access to third party applications.

Google is not a member of BSA, and BSA has no non-public information about the specifications for how Google secures its platform, beyond what can be gleaned from the publicly available literature. However, it is our understanding based on Android's public documentation—and the exemption proponents agree¹—that Google is an open source operating system for mobile devices. *See, e.g.,* <http://source.android.com/> (explaining that “Android is an open-source software stack for mobile devices”). In other words, anyone can use Android—which, according to EFF, is the “best-selling mobile platform in the world”²—for a wide range of purposes. Jailbreaking the iOS or the Windows Phone operating system to install apps, therefore, is a matter of preference, not necessity. Moreover, it is also our understanding based on the publicly available documentation that while Android applications must include a signed certificate, “[t]he certificate does not need to be signed by a certificate authority: it is perfectly allowable, and typical, for Android applications to use self-signed certificates.” <http://developer.android.com/guide/topics/security/permissions.html>. In other words, Android devices are effectively open to a wide range of programs.

¹ See Comments of Electronic Frontier Foundation at p. 4 (describing Android as “a free, open-platform smartphone and tablet operating system”).

² See Comments of Electronic Frontier Foundation at p. 4.

The open platform design of Android is the basis for the Joint Creators' contention—not refuted by EFF—that “Mobile phones and tablets running the Android operating system are available completely unlocked. Although EFF largely ignores this fact, it seriously undermines any need for an exemption in this context.”³

3. At the June 5 hearing, the Business Software Alliance alleged that jailbreaking mobile devices leads to/results in piracy of copyrighted applications. Please discuss the relationship between jailbreaking and piracy, and whether this is relevant to this class of works. In this context, please discuss the accuracy and reliability of the articles and links previously submitted to the Office discussing apps and piracy.

An unlicensed (pirated) copy of an iOS or Windows Phone application will not run on an iPhone or Windows Phone because of the TPMs that require all apps on those devices to be authorized. The only way that a pirated app can have any value to a user is if the user has a “jailbroken” phone – i.e., a device on which the TPM has been removed or disabled. Jailbreaking enables the installation and execution of pirated – i.e., unlicensed – apps on a mobile device. So there is a direct link between piracy and the circumvention of TPMs – jailbreaking is the precondition for making pirated apps valuable. In the case of apps that are sold, the developer is deprived of sales revenue. In the case of apps that are distributed for free, the developer will be harmed if advertisements are stripped out of the unlicensed version of the app, or if the unlicensed version otherwise fails to produce the metrics on which the advertisers' payments to the developer are computed. Either way, the developer is harmed and the incentive to create further copyrighted works is diminished.

BSA does not compile statistics on rates of piracy on mobile devices, so we are unable to quantify it. However, as noted in the articles that BSA and the Joint Creators have previously submitted to the Office, there is a wealth of evidence that piracy of mobile applications is taking place and is having a detrimental effect on some app developers. We have no reason to doubt the accuracy and reliability of those articles.

³ Joint Creators' Comments at p. 22.

Another source of evidence for the existence of piracy on jailbroken devices is the existence of popular repositories – or “repos” – on Cydia that are devoted to pirated iPhone apps (see, e.g., <http://www.se7ensins.com/forums/threads/best-repos-to-get-on-iphone.370844/>; and <http://iphoncaptain.blogspot.com/2011/05/cydia-sources.html>).

Please feel free to contact me if you have further questions.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Jesse M. Feder". The signature is written in a cursive style with a large, stylized initial "J".

Jesse M. Feder
Director of Int'l Trade and Intellectual Property
Business Software Alliance