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

p. 202/872.5500
f .202/872.5501

July 10, 2012

BY EMAIL (1201@loc.gov)
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 following question posed in your letter of June 21, 2012:

> **At the June 5 hearing, questions were raised concerning Microsoft's new Windows 8 operating system and its supposed ability to prevent the unauthorized installation of third party independent operating systems. On this point, the Office referenced an article recently posted on Boingboing entitled "Lockdown: free/open OS maker pays Microsoft ransom for the right to boot on users' computers." See http://boingboing.net/2012/05/31/lockdown-freeopen-os-maker-p.html.**
>
> **In light of this article, please discuss whether and how Windows 8 would prevent another operating system from being installed on a particular computing device.**

BSA appreciates the opportunity to supplement and correct the record and explain why there is no need for the Office to grant any exemption relating to UEFI and Windows 8 secure boot. The proposed exemption should be denied on three independently sufficient grounds.

First, the UEFI secure boot specification is not relevant to these proceedings because the exemption proponents have not demonstrated that it is a "technological measure that effectively controls access to a work protected under this title." The secure boot specification was created by a group of hardware and software companies including Microsoft, Apple, IBM, Dell, and

Intel to combat the massive threat to consumers and businesses posed by malware and viruses.[1] At a high level, secure boot is a specification which prevents malware from loading before the operating system, thereby ensuring the security of the system. Because secure boot exists primarily to prevent the introduction and propagation of malware and viruses, and not to "control[] access to a work protected under this title," proponents have not shown that secure boot is relevant to these proceedings at all.

Second, even if the Office considers the UEFI secure boot specification to be relevant to this proceeding, it is premature at present to evaluate its effect on noninfringing uses. Windows 8 itself is not for sale anywhere, either as packaged software or preinstalled on hardware. Moreover, many of the details regarding Windows 8—including many details about secure boot and UEFI—are confidential and subject to ongoing refinement and development. By definition, therefore, the proponents cannot show that Windows 8 has had an adverse impact on any allegedly noninfringing uses. Any predictions regarding the likely future impact on noninfringing uses would be mere speculation.

Third, the allegation that Windows 8's secure boot blocks other operating systems is not true. The Boingboing article confirms as much, quoting a Linux developer who explains that "[u]sers will retain the freedom to run modified software."[2] But even if it were true it would be irrelevant. There are millions of Intel and ARM devices currently available on the market onto which any operating system can be installed.[3] Even if proponents were correct in their factual assertions (and they are not), the installation of other

---

[1] Additional background information regarding UEFI and its development is available at the UEFI website. *See* http://www.uefi.org/about/. For additional information on the threats posed by malware, *see* Symantec Corporation, "Internet Security Threat Report, Volume 17" (2012), *available at* http://bit.ly/JQNde6.

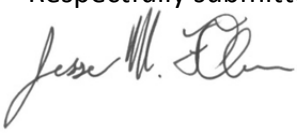
[2] *See also* "Free Software Foundation Recommendations for Free Operating System Distributions Considering Secure Boot" *available at* https://www.fsf.org/campaigns/secure-boot-vs-restricted-boot/whitepaper-web (noting that UEFI merely requires "an additional step" for installation of different operating systems and describing two Linux distributors' plans to enable Linux installations on new hardware); *see also* http://blogs.msdn.com/b/b8/archive/2011/09/22/protecting-the-pre-os-environment-with-uefi.aspx (explaining various ways alternate operating systems may be installed).

[3] As the Linux developer quoted by Boingboing explained, "[i]f you want to run Linux on ARM then there'll be no shortage of hardware available to you."

operating systems on either Intel or ARM devices would be a matter of preference, not necessity.

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

Respectfully submitted,



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