Before the

U.S. COPYRIGHT OFFICE

LIBRARY OF CONGRESS

In the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies

Docket No. RM 2011-7

Comment of the Software Freedom Law Center

Submitted by:
Aaron Williamson
James Vasile
Software Freedom Law Center
1995 Broadway, 17th Floor
New York, NY 10023
(212) 580-0800
(212) 580-0898 (fax)
aaronw@softwarefreedom.org

Pursuant to the Notice of Inquiry of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, the Software Freedom Law Center (SFLC) submits the following comments and respectfully asks that the Librarian of Congress exempt from 17 U.S.C. § 1201(a)(1)'s prohibition on the circumvention of access control technologies, for the period 2012-2015, computer programs that enable the installation and execution of lawfully obtained software on a personal computing device, where circumvention is performed by or at the request of the device's owner.

I. The commenting party

SFLC is a 501(c)(3) nonprofit legal services organization dedicated to protecting and advancing free software.[1] SFLC provides *pro bono* legal representation to developers and educates the public about legal issues affecting free software development. SFLC represents a number of prominent developers and organizations that write and distribute free software directed at personal computing devices, including the Free Software Foundation, which develops and

[1] Free software, also commonly referred to as open source software, is distributed under copyright licenses that allow users to freely run, copy, modify, and redistribute the software. Most free software is also distributed free of charge.

distributes GNU, a collection of free software operating system utilities; the Debian project, which distributes a complete free software operating system based on GNU and Linux; and the Foundation for Free Multimedia Technology, which develops free software commonly used for media playback.

In these comments, SFLC represents the interests of software developers who wish to produce and adapt free software for use on personal computing devices, as well as device owners who seek more control over their personal computing through the use of free software.

II. The proposed class

Computer programs that enable the installation and execution of lawfully obtained software on a personal computing device, where circumvention is performed by or at the request of the device's owner.

III. Summary of argument

In the 2009 rulemaking process, the Librarian granted an exemption to give owners of mobile phones a measure of control over the software running on their phones by allowing them to "jailbreak" their phones from manufacturer and carrier restrictions that prevented the installation and execution of legally obtained software.[2] This exemption recognized an important principle: technological protection measures should not restrict device owners from running whatever software they choose simply because such restrictions serve the manufacturers' interests.

In the intervening years, the restrictions addressed by the 2009 exemption have become commonplace on other mobile computing devices and have begun to appear on personal computers. The 2009 exemption should be expanded to give owners of all personal computing devices the same access to applications as owners of mobile phones have. Also, as a group of independent Android developers have powerfully demonstrated, device owners should have control not only over the applications they use, but over the operating system they use. The 2009 exemption should be expanded to clearly encompass circumvention for the purpose of installing any software the user chooses, including a new operating system.

IV. The factual basis for the exemption

Since the last rulemaking freed mobile phone users to install their choice of applications, the mobile computing market has exploded. Today, nearly 28% of internet users in the United States connect primarily via a mobile device,[3] a category that now includes not just mobile phones but tablets and e-book readers too. These devices have come to heavily supplement or even replace traditional computers for many users. They have also been broadly encumbered by the same restrictions that have plagued mobile phones.

The technological protection measures (TPMs) that restrict these users are of two kinds: those

[2] 37 C.F.R. § 201.40(b)(2) (2010).

[3] Aaron Smith, *Smartphone Adoption and Usage*, Pew Internet & American Life Project, July 11, 2011, http://pewinternet.org/Reports/2011/Smartphones/Section-2/Smartphones-as-an-internet-appliance.aspx.

that prevent the installation and execution of applications that have not been authorized by the manufacturer (“application locks”), and those that prevent the installation and execution of an operating system that has not been authorized by the manufacturer (“OS locks”). These terms each refer to a category of TPMs, rather than a particular technique for restricting users. For example, an “application lock” may prevent a device's owner from running any application that has not been cryptographically signed with the manufacturer's key, as on the Apple iPhone,[4] or it may render some applications inoperable by withholding “root” or administrative access from users, as on Google's Android.[5] Similarly, an “OS lock” may work by preventing the installation of unsigned operating systems[6] or by preventing access to the memory space in which the operating system is installed.[7]

Despite differences in implementation, all application locks effectively prevent users from installing at least some applications and all OS locks effectively prevent users from installing replacement operating systems. Therefore, we refer the various implementations collectively in this document.

A. Computing device makers of all kinds now impose application locks on devices, restricting user control as on mobile phones

In requesting the 2009 exemption, the Electronic Frontier Foundation (EFF) noted that application locks existed in one form or another on the two dominant mobile operating systems of the time, Apple's iOS and Google's Android. Apple's control was total: iPhone owners could only install applications (or "apps") from Apple's iTunes App Store, where Apple maintains arbitrary veto power. Android users were allowed to install applications from channels other than Google's Android Marketplace, but unless certain restrictions were circumvented, those applications had limited access to the phone's functionality.[8]

1. Mobile device makers restrict users of new mobile formats as they do mobile phone users

Today, Android and iOS dominate not only the mobile phone market but the entire mobile device market. Shortly after the 2009 rulemaking, Apple introduced the iPad, a tablet computer running iOS, and kickstarted a new market that has doubled in size for the past several quarters.[9] Google

[4] Greg Kumparak, *Apple Moves to Block Jailbreaking in New iPhones*, TechCrunch, Oct. 13, 2009, http://techcrunch.com/2009/10/13/apple-moves-to-block-jailbreaks-once-and-for-all/.

[5] Robert Strohmeyer, *Root Android the Easy Way*, PCWorld, Sept. 14, 2010, http://www.pcworld.com/businesscenter/article/205336/root_android_the_easy_way.html.

[6] Apple Computer, Inc., Responsive Comment of Apple Inc. in Opposition to Proposed Exemption 5A and 11A (Class #1) at 12, Feb. 2, 2009, available at https://www.eff.org/sites/default/files/filenode/dmca_2009/RM-2008-8.pdf.

[7] Posting of CLShortFuse to http://forum.xda-developers.com/showthread.php?t=803682 (Oct. 9, 2010, 08:56 AM EST). CLShortFuse, the developer of a popular tool to “root” Android devices, explains that “[s]ome devices have a NAND lock which does not allow you to write to [the device's 'system' memory partition].” *Id*.

[8] The Electronic Frontier Foundation, Comment before the U.S. Copyright Office in the matter of exemption to prohibition on circumvention of copyright protection systems for access control technologies, Dec. 2, 2008, https://www.eff.org/sites/default/files/filenode/dmca_2009/RM-2008-8.pdf [*hereinafter* EFF Comment].

[9] *See* Press Release, Apple Computers, Inc., Apple Launches iPad Jan. 27, 2010, http://www.apple.com/pr/library/2010/01/27Apple-Launches-iPad.html; John P. Mello Jr., *Report: Apple's iPad*

followed suit, adapting Android for use on tablets, where it quickly gained market share. Together, iOS and Android devices now account for 94% of this rapidly expanding market.[10] Android's dominance extends even beyond tablets: the latest models of the two most popular e-book reader devices, Amazon's Kindle and Barnes & Noble's Nook, are Android-based devices.[11]

All of the restrictions addressed by the 2009 exemption are reproduced on the new formats. As on the iPhone, iOS on the iPad prevents the installation of any applications except via the App Store. Android tablets and e-book readers, like Android phones before them, withhold many vital privileges from user-installed applications. The Amazon and Barnes & Noble e-book readers substitute Google's exclusive application distribution system, the Android Market, with their own exclusive channels that cannot be circumvented without jailbreaking. Even as these restrictions have been copied and pasted from mobile phones to tablets and e-book readers, the 2009 exemption has remained limited to mobile phones, leaving owners of other devices vulnerable to claims under 17 U.S.C. § 1201(a)(1).

2. Personal computer operating system vendors will soon use application locks to restrict PC users

The app store distribution model popularized by iOS and Android—a single, vendor-controlled source for approved applications—is a marked deviation from how software has historically been distributed for personal computers. Until recently, most people either purchased software from a retailer (physical or online) or downloaded it directly from its developer or publisher.

While the app store model offers users some new conveniences, it also places unprecedented control in the hands of the store's owner. Apple uses this control to exclude competition, squelch criticism, and censor content.[12] Both Apple and Google use it to collect a percentage from the sale of each and every application.[13]

Recently, Apple and Microsoft, who together control nearly the entire PC operating system market,[14] have introduced app stores for their respective PC operating systems that closely follow the model of their mobile predecessors. These PC app stores (the Mac App Store and the Windows 8 Store, respectively) are not yet the sole distribution channel for either operating system, but Microsoft at least is moving quickly to make the Windows 8 Store exactly that. It has already announced plans to divide Windows 8 applications into two classes: next-generation

Dominance Fades, PCWorld, Oct. 21, 2011, http://www.pcworld.com/article/242360/report_apples_ipad_dominance_fades.html.

[10] *See* Mello, *supra* note 9, at 3.

[11] Phil Wahba, *Barnes & Noble sees strong Nook growth,* Reuters, Aug. 30, 2011, http://www.reuters.com/article/2011/08/30/us-barnesandnoble-idUSTRE77T2AZ20110830.

[12] EFF Comment, *supra* note 8, at 5-6; Alicia Eler, *The Other Steve Jobs: Censorship, Control, and Labor Rights*, ReadWriteWeb, Oct. 5, 2011, http://www.readwriteweb.com/archives/the_other_steve_jobs_censorship_control_walled_gar.php.

[13] EFF Comment, *supra* note 8, at 6; Android Market for Developer Help—Transaction Fees, http://www.google.com/support/androidmarket/developer/bin/answer.py?&&answer=112622 (last visited Dec. 1, 2011).

[14] Wikipedia—Usage share of operating systems, https://en.wikipedia.org/wiki/Usage_share_of_operating_systems (last visited Dec. 1, 2011).

applications employing Windows 8's new "Metro" interface can be sold only through the Windows 8 Store, while last-generation applications can still be installed without approval from Microsoft.[15] Beginning in March, Apple will begin severely restricting the functionality of applications distributed via the Mac App Store, much as iOS and Android applications are restricted now.[16]

As on tablets and e-book readers, the expansion of the app store model has brought to personal computers the restrictions addressed by the 2009 exemption. If the exemption is not expanded accordingly, these restrictions threaten to give operating system vendors monopolistic control over application development and distribution on what have previously been unrestricted platforms that engendered competition in the market and enabled user control.

B. Operating system locks harm users

The 2009 exemption addresses application locks; it deals with OS locks only insofar as replacing the operating system with a slightly modified one is necessary to circumvent an application lock. It does not clearly permit circumvention of an OS lock solely for the purpose of replacing the operating system.[17] But operating system locks are even more prevalent in the mobile device market than application locks. While many mobile operating systems (including Apple's iOS, Palm's WebOS, and Microsoft's Windows Phone OS) prohibit unauthorized applications, the most popular mobile operating system (Google's Android) does not. By contrast, nearly every mobile phone on the consumer market, including most Android phones, prevents the installation of unauthorized operating systems via a TPM.

The 2009 exemption should be extended to reach operating system locks because these restrictions adversely affect consumers exactly as application locks do: they impede competition, consumer choice, and innovation in the operating system software market. They also contribute to the premature obsolescence of consumer electronics devices, contributing to environmental degradation and poor working conditions in the factories that produce them.

1. Operating system locks impede alternative operating systems for devices

The stated justification for operating system locks is to protect device owners from malicious software:[18] to make it impossible for viruses and other malware to gain access to, exploit, or replace any portion of a device's operating system. Unfortunately, this “security feature” is undiscerning: it will reject the device owner's intentional installation of an operating system just as it will reject a virus's payload.

[15] Adrian Kingsley-Hughes, *Windows 8: App Store will be the only source of Metro apps*, ZDNet, Sept. 19, 2011, http://www.zdnet.com/blog/hardware/windows-8-app-store-will-be-the-only-source-of-metro-apps/14873.

[16] David W. Martin, *OS X Lion Sandboxing*, Cult of Mac, Nov. 7, 2011, http://www.cultofmac.com/113977/os-x-lion-sandboxing-is-a-killjoy-destined-to-ruin-our-mac-experience/.

[17] 37 C.F.R. § 201.40(b)(2) (2010) (permitting circumvention “for the sole purpose of enabling interoperability of... applications... with computer programs on the telephone handset”).

[18] Chris Ziegler, *Motorola responds to Droid X bootloader controversy, says eFuse isn't there to break the phone*, Engadget, July 16, 2010, http://www.engadget.com/2010/07/16/motorola-responds-to-droid-x-bootloader-controversy-says-efuse/.

In practice, OS locks are used not only to protect the user from malware, but to prevent the user from removing spyware intentionally installed by the manufacturer.[19] This malicious software, which reports a user's activity to the carrier or manufacturer, is itself a security risk and a significant privacy intrusion. iOS and Android phones continuously (and often secretly) report their users' physical location to Apple or Google.[20] As typically configured by Google and its partners, Android funnels a huge portion of a user's communications through Google's servers, giving Google access to most of a user's important interactions. The only way to definitively disable all such tracking is to replace the preinstalled operating system with a free software version that is verifiably free of spyware.

Despite the near-ubiquity of OS locks, many users have replaced their mobile devices' operating systems. This is particularly common among Android users: beginning around the time of the 2009 rulemaking, a flourishing community emerged around the development and trading of operating systems based on Android. This activity is noninfringing because the fundamental components of Android are licensed under free software licenses, which permit users to distribute modified versions of the operating system (modified mobile operating systems are commonly referred to as "mods" and the people who make them as "modders"). The most popular Android mod, CyanogenMod, has been installed nearly 700,000 times.[21] But even though these mods are licensed by the copyright owner, the users who install them do so under the specter of § 1201(a)(1) liability, because the vast majority of handsets capable of running Android employ OS locks.

Some of these users replace their device's default operating system to access applications that are otherwise unavailable to them, as the Librarian recognized in 2009. But there are other good reasons to use a mod. One is to remove the manufacturer's hidden spyware. Another is to gain access to features of the *operating system* that are unavailable in the default firmware. Mods regularly introduce features called for by consumers months or even years before they are integrated into the corresponding default operating system.[22] Mods also enable access to features, like tethering, that carriers prefer to disable.[23]

This constant innovation by modders introduces important competition into the market for mobile operating system features. Absent mods, some feature competition exists *between*

[19] *See* David Kravets, *Researcher's Video Shows Secret Software on Millions of Phones Logging Everything*, Wired, Nov. 29, 2011, http://wired.com/threatlevel/2011/11/secret-software-logging-video/last visited.

[20] *See* Julia Angwin and Jennifer Valentino-Devries, *Apple, Google Collect User Data,* Wall Street Journal, Apr. 22, 2011, http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html.

[21] CyanogenMod—CMStats , http://stats.cyanogenmod.com/ (last visited Nov. 29, 2011).

[22] For example, a modification to iOS introduced an improved "alert notification" system over three months before a nearly identical feature was announced by Apple. *See* Devindra Hardawar, *Apple's iOS 5 notifications sure look familiar*, Mobile Beat, Jun. 7, 2011, http://venturebeat.com/2011/06/07/mobilenotifier-ios-5/. An Android modder enabled multitouch capabilities on Android six months before Google did. *Compare* Chris Davies, *T-Mobile Multitouch Mod Released*, Slash Gear, Jan. 26th 2009, http://www.slashgear.com/t-mobile-g1-multitouch-mod-released-video-demo-2631875/ *with* Chris Davies, *Google Release Android 2.0 Donut with CDMA and Multitouch*, Slash Gear, Jul. 26, 2009, http://www.slashgear.com/google-release-android-2-0-donut-with-cdma-and-multitouch-2650318/.

[23] Mike Isaac, *Carriers Crack Down on Wireless-Tethering App for Android*, Wired, May 2, 2011, http://www.wired.com/gadgetlab/2011/05/wireless-tethering-crackdown/.

platforms, but the cost to consumers of switching between platforms is prohibitive: mobile phones are only affordable to most consumers because they are heavily subsidized by carriers; customers who wish to switch phones or carriers before their subsidy period (typically 2 years) expires will face heavy penalties.[24] By contrast, mods introduce *intraplatform* competition, allowing consumers to choose the best operating system for the phones they already own.

An exemption for circumventing OS locks is needed not only so that users can install modified versions of their devices' default operating systems—at present, Android is the only mass-market mobile operating system that permits modification—but so that users can install *any* operating system they choose to. In the relatively open personal computing environment, dozens of community-developed free software operating systems compete with the dominant vendors, Microsoft and Apple, providing users genuine, free-of-cost alternatives to the operating systems preinstalled on their computers. While similar efforts for mobile devices are, like the industry itself, relatively young, there are several projects working on free software operating systems for mobile devices, including the Mer Project[25] and freesmartphone.org.[26] But the viability of these and other community-produced operating systems depends on the availability of hardware to run them on. Unlike in the PC market, there are as yet no producers of commodity mobile phone hardware. Nearly all modern handsets are produced by vendors with ties to proprietary operating system vendors: Nokia to Microsoft; Motorola, HTC, and others to Google. (Apple and RIM control production of both the hardware and the operating systems for their devices.) Without an exemption, mobile device owners cannot choose a free software operating system without fear of liability, and consequently these alternatives may never receive the community participation they need to become truly competitive.

2. Operating system locks contribute to early obsolescence

Enabling users to install the operating system of their choice extends the useful life of devices. Rapid obsolescence plagues the mobile computing sector: new phone models are introduced relentlessly, often showcasing a newer version of the corresponding operating system.[27] While the hardware from one model to the next typically changes only incrementally, changes to the operating system often introduce desirable new features.[28] But when a new version of iOS or Android is released, updates are made available for previous model phones only selectively, if at all. Whether this neglect is motivated by profit (i.e. to drive consumers to upgrade) or by other considerations, the result is the same: previous models fall behind the state of the art despite having perfectly capable hardware. The failure to update previous models also exposes owners of those models to security risks, because new versions of operating systems don't just introduce new features, they also fix security holes in prior releases. This problem is widespread: nearly

[24] *See, e.g.*, John Paczkowski, *AT&T's New Early-Termination Fee for the iPhone: $325*, AllThingsD, May 21, 2010, http://allthingsd.com/20100521/att-jacks-smartphone-early-termination-fee-to-325/.

[25] Mer Project, http://www.merproject.org/ (last visitedlast visited Nov. 29, 2011).

[26] Freesmartphone.org, http://www.freesmartphone.org/ (last visitedlast visited Nov. 29, 2011).

[27] *See* Wikipedia—Comparison of Android devices, https://en.wikipedia.org/wiki/Comparison_of_Android_devices (last visited Dec. 1, 2011) (listing hundreds of Android devices released between Oct. 22, 2008 and today).

[28] For example, Apple's Siri personal assistant application is only available on the latest iPhone model. Kyle Wagner, *Siri Personal Assistant Only Works on the iPhone 4S*, Gizmodo, Oct. 4, 2011, http://gizmodo.com/5846550/apples-siri-personal-assistant-only-runs-on-the-iphone-4s.

every Android phone ever released was abandoned by its manufacturer less than *one year* after its release.[29]

Lifting the prohibition on replacing mobile operating systems would enable users to extend the life of their devices in two ways: by upgrading to the latest version of the default operating system, when no upgrade is made available by the manufacturer, and by replacing the default operating system on an older device entirely with another, less resource-intensive one. This is common practice for desktop and laptop computer owners. A number of modern operating systems, most of them free software, are designed specifically to run on older hardware.[30] Organizations like Free Geek refurbish donated PCs, many of which are too slow to capably run the latest version of Windows or Mac OS X, then outfit them with a greener Linux-based operating system and give them to people in their communities.[31] This repurposing enables more people to afford computing devices with modern software and keeps devices out of landfills. Enabling the replacement of mobile operating systems would produce similar benefits.

3. OS locks threaten user choice in the PC market

Locked firmwares first became prevalent on mobile phones; from there they spread quickly to the rest of the mobile device market. On tablets as on mobile phones, manufacturers opted overwhelmingly to prevent the replacement of the default operating system, using OS locks.[32] And as on mobile phones, these locks have discouraged the use of alternative operating systems on the locked devices.

A similar fate threatens personal computers: a majority of new laptop and desktop personal computers shipped in the next year are expected to incorporate hardware controls that allow manufacturers to prevent the installation of unauthorized operating systems. In theory, these controls will merely make it difficult, but not impossible, for a user to install their choice of operating system. In practice, however, there is a very real danger that the controls will impose an OS lock on many personal computers.

In April 2011, a trade association called the UEFI Forum introduced version 2.3.1 of the Unified Extensible Firmware Interface, a standard that defines how an operating system interfaces with the hardware platform on which it runs.[33] The new version of UEFI includes a feature called "secure boot" which can be used as an OS lock to prevent the installation of an unauthorized operating system. Microsoft has announced that it will require hardware manufacturers that wish to participate in its Windows 8 Logo Program (a certification that a particular computer is

[29] Michael Degusta, *Android Orphans: Visualizing a Sad History of Support*, theunderstatement, Oct. 26, 2011, http://theunderstatement.com/post/11982112928/android-orphans-visualizing-a-sad-history-of-support.

[30] Jeff Orloff, *Linux: Lean, clean, and green*, IBM developerWorks, May 26, 2009, http://www.ibm.com/developerworks/linux/library/l-green-linux/index.html.

[31] Freegeek, http://www.freegeek.org/ (last visited Nov. 29, 2011).

[32] *See, e.g.*, Michael Crider, *Nook Tablet owners frustrated over 1GB storage, locked bootloader*, AndroidCommunity, Dec. 1, 2011, http://androidcommunity.com/nook-tablet-owners-frustrated-over-1gb-storage-locked-bootloader-20111201/.

[33] Wikipedia—Extensible Firmware Interface, https://en.wikipedia.org/wiki/Extensible_Firmware_Interface (last visited Dec. 1, 2011).

compatible with Microsoft's latest operating system) to enable secure boot by default.[34] Since Microsoft controls nearly 90% of the operating system market,[35] most major hardware vendors participate in the Logo Program, meaning this requirement will make UEFI secure boot nearly ubiquitous on new personal computers in the next year.

In the mobile device market, firmware locks have largely prevented the emergence of viable alternative operating systems. But in the PC market, such alternatives are legion. Wikipedia lists over 200 unique notable GNU/Linux-based operating systems,[36] and around 80 operating systems based on the Berkeley Systems Distribution, another popular free software operating system.[37] The widespread introduction of OS locks into this thriving ecosystem could decimate the existing competition.

The UEFI specification does not define a means for users to disable the OS lock, only how it will operate when enabled: it requires a secure boot-enabled machine to load only an operating system that corresponds to an approved cryptographic signature in the machine's firmware. The easiest way for a manufacturer to implement the specification as required by the Windows Logo Program is to include only Microsoft's key in the firmware. The specification does not prevent manufacturers from allowing users to disable the lock or add non-Microsoft keys, but neither does it require or encourage them to, and market incentives discourage it: since Windows is used on about 99% of non-Apple personal computers, there is little incentive to provide for other operating systems.[38]

It is no solution for producers of free software operating systems to merely provide their own keys to hardware manufacturers. An important strength of free software is that it is not subject to centralized control. The nearly 300 GNU/Linux- and BSD-derived operating systems referenced above are by and large produced by distinct communities of developers, without the support or control of any company or formal entity. Most of these community development groups have neither the resources nor the clout to negotiate with manufacturers to include their keys in new hardware. A manufacturer-controlled whitelist, therefore, would at best privilege well-resourced commercial GNU/Linux distributions along with Windows over less prominent distributions. Moreover, new free software operating systems are introduced regularly; if users cannot install them on existing secure boot-enabled machines due to the OS lock, they have no hope of competing.

While the least-cost implementation of the secure boot OS lock could have devastating results for free software operating systems, an exemption to mitigate this potential harm would have no

[34] Arie van der Hoeven, Principal Lead Program Manager, Microsoft Corporation, Address at Microsoft Build Windows Event (Sept. 14, 2011), video available at http://channel9.msdn.com/Events/BUILD/BUILD2011/HW-457T.

[35] John Broadkin, *Windows Drops Below 90% Marketshare*, NetworkWorld, Feb. 2, 2011, http://www.networkworld.com/community/blog/windows-drops-below-90-market-share.

[36] Wikipedia—List of Linux Distributions, https://en.wikipedia.org/wiki/List_of_Linux_distributions (last visited Dec. 1, 2011).

[37] Wikipedia—List of BSD operating systems, https://en.wikipedia.org/wiki/List_of_BSD_operating_systems (last visited Dec. 1, 2011).

[38] Wikipedia—Usage share of operating systems, https://en.wikipedia.org/wiki/Usage_share_of_operating_systems (last visited Dec. 1, 2011).

ill effects. The exemption would merely affirm the freedom that all personal computer owners now have, to decide what software to run on hardware they own. This is fundamentally the same right that the Librarian recognized in 2009, when he exempted jailbreaking of mobile phones. As the technology that "jailed" mobile phone users spreads to other formats, the Librarian should recognize that the owner of any personal computing device should be free to install the software of his or her choice.

This exemption would not undermine the stated purpose of OS locks, to protect users from malicious tampering with the operating system. It would merely enable users to make an informed choice about whether the "protected" default operating system was the right one for them. Manufacturers and operating system vendors would not be harmed; they already can (and do) limit warranties such that harm caused by modification of the operating system is not covered.[39] The exemption merely ensures that, should OS locks obstruct users from installing whatever software they choose on devices they own, they will not be subject to DMCA liability for removing the obstruction.

V. Legal arguments in support of the exemption

A. Replacing a preinstalled operating system is not infringement

The Librarian's request for comments says that "a proponent should establish that the prevented activity is, in fact, a noninfringing use under current law." As the Register concluded in recommending the 2009 exemption, it is not infringing for the owner of a device to install applications that have not been approved by the device's manufacturer.[40] The Register's analysis and findings there apply with equal force to application locks on devices other than mobile phones; it would be duplicative to repeat them here. As with application locks, enabling device owners to circumvent OS locks to install licensed operating systems would not promote infringement.

The 2009 exemption implicitly recognized the noninfringing purpose of circumventing OS locks. The Register found that, to enable interoperability between third-party applications and the preinstalled operating system, it would sometime be necessary to modify the phone's operating system, which requires circumvention of the OS lock. Nonetheless, the Register concluded that, to the extent such use was necessary to circumvent application locks, it was either noninfringing or fair.

While modification of the preinstalled operating system is sometimes necessary to circumvent an application lock, the same is not true of OS locks: removal of a device's default operating system does not require its reproduction, derivation, distribution, performance, or display, and so cannot infringe any 17 U.S.C. § 106 right of the operating system's copyright holder. The installation and execution of an alternative operating system implicates only the rights of the copyright

[39] *E.g.*, Daniel Ionescu, *Never Mind Legality, iPhone Jailbreaking Voids Your Warranty*, PCWorld, July 27, 2010, http://www.pcworld.com/article/201968/never_mind_legality_iphone_jailbreaking_voids_your_warranty.html.

[40] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 37 C.F.R. § 201.

holder in that operating system. Since the proposed exemption only permits circumvention for the purpose of installing a licensed operating system, this use is by definition non-infringing.

B. There are no alternatives to circumvention

The Librarian's request for comments directs commenters to "demonstrate why the access-protected copy of a work is needed for the noninfringing use." To run an alternative operating system on a locked device does not require any *use* of the access-protected operating system. However, it must be removed so that the alternative operating system can be installed in its place. To the extent the firmware lock being circumvented merely prevents unauthorized operating systems from running, it does not protect access to a copyrighted work of the device producer, but rather prevents access to a competing copyrighted work to which the device owner has a license.

Device owners cannot avoid circumvention merely by purchasing devices that are not locked. In the case of mobile phones, this is a practical impossibility; nearly every one ever produced employs some form of OS lock. While a few models of Android phone have been sold "unlocked," these have been marketed primarily to software developers and unlike most models, do not qualify for the carrier subsidies without which most consumers cannot afford mobile phones.[41] The situation on tablets and other mobile devices is much the same; in the PC market, it soon may be.

C. The exemption is favored by the statutory considerations

The Register of Copyrights is directed to consider the following when evaluating a proposed exemption: "(i) The availability for use of copyrighted works; (ii) the availability for use of works for nonprofit archival, preservation, and educational purposes; (iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research; (iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and (v) such other factors as the Librarian considers appropriate."[42] Each of these factors favors the exemption.

1. The exemption will give device owners greater access to copyrighted works

The sole purpose of this exemption is to increase the availability of copyrighted works for use on personal computing devices. It will give owners of all devices the same right mobile phone owners have to choose where they get applications; it will expand their access to operating systems in the same way. The operating systems available for use on mobile devices dramatically limited at the discretion of device manufacturers and (in the case of mobile phones) network carriers. OS locks enforce the manufacturer's initial choice of operating system, leaving users with no alternatives if that choice proves poor or if, as is overwhelmingly the case on Android phones, the carrier abandons a user's device in favor of later models. An exemption would

[41] Priya Ganapati, *Google Offers Unlocked Nexus One to Devleopers*, Wired, August, 5, 2010, http://www.wired.com/gadgetlab/2010/08/google-unlocked-nexus-one/.

[42] 76 Fed. Reg. 60398, 60403 (Sept. 29, 2011).

expand the availability of operating systems in two dimensions: it would enable users to upgrade to newer versions of their default operating system, when such upgrades are not made available by the manufacturer; it would also enable users to install entirely different operating systems on their devices.

Without this exemption, community-built free software operating systems have little chance of succeeding on locked platforms. Because the communities that build these operating systems do not have the organization or clout to make deals with manufacturers, their products can only become competitive if users choose to install them as aftermarket replacements. The success of the GNU/Linux operating system demonstrates that community-developed operating systems depend on open access to computing platforms to attain broad user bases and compete with commercial, proprietary operating systems. OS locks threaten to block that access, just as community-developed mobile operating systems are poised to have significant impact. Hundreds of thousands of users have installing a new operating system on their mobile device. The threat of civil liability hampers their efforts as well as the ability to share information about their techniques and experiences. As a result, many people who would like to take control of the operating system and software on their phones cannot do so. As UEFI secure boot is implemented on a majority of new PCs over the next year, these same restrictions will threaten users there as well.

2. The exemption encourages the educational use of certain works

The availability of free software operating systems on existing mobile devices would serve important educational purposes. Because free software is available in source-code form, students and researchers can study and learn from existing implementations. And because it is licensed such that anyone can copy, modify, and redistribute it, it can serve as the foundation of new research and development, saving researchers valuable time and effort.[43] As mobile computing gains prominence, this exemption would enable scholarship to keep pace by allowing students and researchers to test their research on existing devices.

3. Application and OS locks repress criticism, comment, teaching, scholarship, and research

Apple has repeatedly used its control over the App Store to squelch criticism and to censor content it disapproves of. Not three months ago, it banned *Phone Story*, a game that illustrates the problems with Apple's (and other manufacturers') real-world supply chain:[44] the exploitation of children and other laborers in military-controlled Congolese Coltan mines; the punishing working conditions and high suicide rate at the Shenzhen factories of Foxconn, where iPhones are produced; Apple's marketing model of planned and perceived obsolescence, by which previous product models are rapidly superseded by new models; and the troubling volume of toxic waste produced by the consumer electronics industry every year.[45]

[43] *See generally* Ralph Morelli et al., *Revitalizing Computing Education Through Free and Open Source Software for Humanity,* 52 Communications of the Association for Computing Machinery 67 (2009).

[44] Eler, *supra* note 12.

[45] Phone Story Home Page, http://phonestory.org/index.html (last visited Dec. 1, 2011).

Apple bans not only applications critical of its methods, but also those that offend its sensibilities: it has banned several applications that contain nudity (including a comic-book adaptation of James Joyce's *Ulysses*, which Apple has since allowed in the App Store in response to public outcry) and depictions of violence.[46] An exemption that permits all device owners to circumvent application locks would allow users, not Apple, to choose what content is appropriate for them.

Both application and OS locks stifle practical computer science research. Mobile computing platforms are now of enormous commercial and social importance and have become a focus of computer science research.[47] Unless computer scientists and students can test their research on commercially available devices, innovation in the field of operating systems will become (and in the case of mobile devices, remain) the province of wealthy businesses.

4. The exemption favors competition and choice in the market for operating systems and applications

As EFF showed in its application for the 2009 exemption, Apple uses its control over the sole iOS application distribution channel to restrain competition.[48] This control now extends to the iPad as well as the iPhone. An exemption that applies to all computing devices will simply extend the choice now available to mobile phone users to owners of all kinds of devices.

The exemption for circumvention of OS locks would not diminish the market for existing mobile operating systems. As the Librarian found in granting the "jailbreaking" exemption, end users do not pay for mobile operating systems separately from the devices on which they're initially installed. Since carriers include some operating system on every handset whether or not users are allowed to replace it, the market for OEM operating systems will continue to be equal to the market for handsets.[49]

As for alternative operating systems and applications, the exemption would greatly increase their value. These products are useless if they are locked out of devices and computers. Breaking the locks expands the market for alternatives, which enhances the value of those alternatives.

[46] *Id*.

[47] *See, e.g.*, Press Release, Lafayette College, Computer Science Students Produce Software that Could Change the Way Geologists Work in the Field (Nov. 4, 2011).

[48] EFF Comment, *supra* note 8, at 5-6.

[49] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 37 C.F.R. § 201.