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. 2014-07

Petition of Electronic Frontier Foundation

Submitted by:

Electronic Frontier Foundation
Mitchell L. Stoltz
Corynne McSherry
Kit Walsh
815 Eddy St
San Francisco, CA 94109
(415) 436-9333
mitch@eff.org

The Electronic Frontier Foundation submits the following petition and respectfully asks the Librarian of Congress to exempt the class of copyrighted works described below from 17 U.S.C. § 1201(a)(1)'s prohibition on the circumvention of access control technologies for 2015-2018:

Proposed Class: Computer programs that enable mobile computing devices, such as telephone handsets and tablets, to execute lawfully obtained software, where circumvention is accomplished for the sole purposes of enabling interoperability of such software with computer programs on the device, or removing software from the device.[1]

I. The Commenting Party

The Electronic Frontier Foundation (EFF) is a member-supported, nonprofit public interest organization devoted to maintaining the traditional balance that copyright law strikes between the interests of copyright owners and the interests of the public. Founded in 1990, EFF represents thousands of dues-paying members, including consumers, hobbyists, computer programmers, entrepreneurs, students, teachers, and researchers, who are united in their reliance on a balanced copyright system that ensures adequate protection for copyright owners while facilitating innovation and broad access to information in the digital age.

[1] Petitioners expect to further develop the proposed exemption consistent with the principles identified in this petition and the record developed in the course of this proceeding.

II. Proposed Class: Jailbreaking

The proposed exemption applies to circumvention of the technical protection measures included in a mobile computing device's firmware that restrict the use of lawfully obtained software (known as "jailbreaking" or "rooting"),[2] in order to run lawfully acquired software that is otherwise prevented from running. Mobile device users jailbreak for a variety of reasons, such as to install the latest fixes for security vulnerabilities, to keep the software on a device current after the manufacturer has stopped supporting it, and to run many kinds of important and useful software excluded by the manufacturer. Jailbreaking requires modifying the firmware on a device, and sometimes making temporary copies of the firmware to accomplish the modification. These are non-infringing fair uses of the computer programs involved. This exemption is not intended to apply to computer programs running on devices designed primarily for the consumption of a single type of media, such as dedicated e-book readers, nor to programs running on desktop or laptop computers.

The Librarian has granted an exemption for software on mobile phones in each of the last two triennial proceedings. In this proceeding, we ask the Librarian to create an equivalent exception and extend it to software running on the family of devices that are sold with mobile operating systems such as iOS, Android, and Windows Phone.

III. Copyrighted Works Sought to be Accessed: Computer Programs on Mobile Computing Devices

The copyrighted works at issue are computer programs that run on mobile computing devices such as smartphones and tablets. Mobile devices have surpassed PCs as the dominant form of personal computing equipment. As of April 2014, almost 170 million people in the U.S. owned a smartphone.[3] Large-format phones that also function as tablets (known as "phablets") are expected to sell 175 million units in 2014, exceeding sales of portable PCs (i.e., laptops).[4]

Mobile computing devices are recognized by manufacturers, consumers, and policymakers alike as a distinct product category, separate from PCs and from single-purpose media consumption devices such as e-book readers, handheld video game devices, and basic personal music players.[5]

---

[2] Modification of firmware to allow installation of other software will be referred to generally as "jailbreaking" in this Petition, although "rooting" is the preferred term for Android devices.

[3] http://www.comscore.com/Insights/Press-Releases/2014/6/comScore-Reports-April-2014-US-Smartphone-Subscriber-Market-Share.

[4] http://www.idc.com/getdoc.jsp?containerId=prUS25077914.

[5] http://www.consumerreports.org/cro/video-hub/electronics/computers--internet/tablet-vs-laptop/16952110001/1178368925001/; *In the Matter of Motorola Mobility LLC, and Google Inc.*, File No. 1210120, Complaint, *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130724googlemotorolacmpt.pdf. (Categorizing computing devices as "mobile phones, tablet computers, and 'smart' devices providing internet access such as gaming systems, laptops, and set-top boxes.").

New types of mobile computing devices have begun to appear on the market as well, particularly wearable devices such as smart watches and smart eyewear. These devices run the same mobile operating systems as phones and tablets, particularly Android and iOS. Like phones and tablets, they are general purpose computers for which many people seek to run alternative software.

Unlike PC users, mobile device users obtain much of their software through "app stores" run by the device manufacturer or the operating system developer. The major app stores distribute millions of software programs. However, a great volume and variety of software written for mobile devices is lawfully sold and distributed through other channels, including alternative software markets and directly on the Internet. For example, an alternative open source firmware for Android devices called CyanogenMod had over 10 million users as of December 2013.[6] For iOS devices, the alternative software market Cydia is used by more than 23 million devices in the U.S.[7]

IV. Technological Protection Measure: Firmware Restrictions on Loading or Running Software

Nearly all mobile computing devices sold in the U.S. contain technological measures that restrict the loading and running of lawfully acquired software. These measures include cryptographic verification in a device's "bootloader" – the program that runs at device startup – that stop alternative or modified operating systems from running. They also include access controls within the operating system that limit what software can do, or prevent some software from running.

For example, Apple, Inc.'s iOS operating system, which runs the iPhone, iPad, and iPod Touch, blocks all software from running on those devices unless the software is cryptographically signed by Apple. This means that, without circumvention, only software approved by Apple for sale in its iTunes Store can run. Smartphones running iOS comprise 42.1% of the smartphones in use in the U.S. as of June 2014, and 51% of the tablet market.[8] With respect to Android, access controls within the operating system, referred to by programmers as restrictions on "root" access, prevent software running on the device from performing many functions. Firmware on Android devices also prevents installing an alternative operating system. Bypassing these restrictions requires "rooting" a device by circumventing one or more security mechanisms.

V. Noninfringing Uses: Modifying the Firmware To Allow Software to Load and Run

A. The Proposed Class Targets Lawful and Useful Activities

Mobile device users seek to circumvent these access controls in order to run lawfully acquired software that is otherwise barred from running. There are many excellent reasons to do so. For example, the restrictions built into Android block many software programs that function as a firewall to prevent leakage of personal information by other applications, and many forms of

---

[6] http://www.androidpolice.com/2013/12/22/cyanogenmod-is-now-installed-on-over-10-million-android-devices/.

[7] http://thenextweb.com/apple/2013/03/02/popular-jailbreak-software-cydia-hits-14-million-monthly-users-on-ios-6-23-million-overall/ (2013 data).

[8] http://www.comscore.com/Insights/Market-Rankings/comScore-Reports-June-2014-US-Smartphone-Subscriber-Market-Share; http://tabtimes.com/resources/the-state-of-the-tablet-market (2013 data).

virtual private network (VPN) software that encrypt data in transit. Android owners are also prevented from *removing* unwanted software installed by the manufacturer – often software that consumes energy, shortens the device's battery life, or sends personal information to advertisers.

Apple device owners face even more restrictions. For example, Apple's iTunes Store rejects "objectionable or crude" applications,[9] and programs with marijuana-related content,[10] among many other categories. Apple device owners are also barred from installing many new and interesting software programs that haven't been approved by Apple for any number of reasons, such as when a program competes with an Apple product.

In addition, mobile device manufacturers are often slow to distribute new operating system versions and fixes for security vulnerabilities to device owners. This means that device owners are often left vulnerable until their manufacturer or mobile carrier distributes a fix, often only once or twice per year. Jailbreaking allows owners to install fixes much sooner.

B. Jailbreaking and Rooting Are Lawful Fair Uses

Loading and running lawfully acquired software on a computing device is a fair use under 17 U.S.C. § 109, as the Librarian concluded (regarding smartphones) in two prior rulemakings.[11]

Under the first factor, copying and modification of code to achieve interoperability of software is a purpose favored by copyright law. Caselaw overwhelmingly supports the Librarian's prior conclusion that allowing device owners to use new software on a computing platform is a favored purpose.[12] Modifying software on one's own device is noncommercial, adding further weight to the first factor.

The second factor, the nature of the copyrighted work, is particularly important in cases involving software interoperability, because software is functional as well as creative. The modifications that constitute jailbreaking concern only the functional aspects of the device firmware,[13] and permitting copyright to restrict such modifications would create "a de facto monopoly over the functional aspects" of the work.[14] Thus, the second factor also favors fair use.

The third factor examines the amount of the work used in an effort to determine whether the "quantity and value of the materials used are reasonable in relation to the purpose of the copying."[15] Where software is modified for purposes of interoperability, copying the entire work

---

[9] https://developer.apple.com/appstore/resources/approval/guidelines.html.

[10] *Available at:* http://arstechnica.com/gaming/2014/05/apple-pulls-popular-weed-growing-game-from-app-store/.

[11] Register's Recommendation in RM 2008-8, June 11, 2010 ("2010 Recommendation") at 103; Register's Recommendation in RM 2011-7, Oct. 12, 2012 ("2012 Recommendation") at 76-77.

[12] *See Sega, LTD. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992); *Sony Computer Entm't v. Connectix Corp*., 203 F. 3d 596 (9th Cir. 2000); *see also Kelly v. Arriba Soft Corp.,* 336 F. 3d 811 (9th Cir. 2003), *Perfect 10, Inc. v. Amazon, Inc.*, 508 F.3d 1146 (9th Cir. 2007).

[13] 2012 Recommendation at 73.

[14] *Sega*, 977 F.2d at 1526.

[15] *Campbell v. Acuff Rose Music, Inc*., 510 U.S. 569, 586-87 (1994).

is sometimes necessary.[16] While the amount of firmware that must be copied in order to jailbreak a device varies between devices, this factor still favors fair use if the user copies only what is necessary for that purpose.[17]

The fourth factor considers the direct harms caused by a particular use on the market or value of a work.[18] Jailbreaking and rooting device firmware do not foreclose any sales of the firmware, or harm its sale or licensing. Indeed, the market for smartphones and their firmware has grown exponentially in the four years since the Librarian first granted a jailbreaking exemption, and the tablet market has also shown explosive growth despite the availability of jailbreaks.

All four factors continue to support the finding that jailbreaking mobile computing devices for the purpose of installing lawfully acquired software is noninfringing.

VI. Adverse Effects of the Prohibition on Circumvention

A prohibition on circumvention restricts mobile computing device users to software approved by the device manufacturer, chilling users from engaging in the numerous lawful and important activities outlined above. A user who wishes to protect her security, make her device more efficient, or access applications not approved by the manufacturer, faces legal risk.

In the 2009 and 2012 rulemakings, the Register of Copyrights recognized that the § 1201 circumvention ban was established to foster the availability of copyrighted works in the digital environment, and agreed that the prohibition on smartphone "jailbreaking"—the practice of enabling the phone to become interoperable with unauthorized independently created applications—was "adversely affecting the ability to engage in the non-infringing use of adding unapproved, independently created computer programs to their smartphones."[19]

That same conclusion holds true today, for all mobile computing devices. A vibrant and innovative community has emerged to provide users with alternatives to the offerings "approved" by mobile device manufacturers. Absent a continued and expanded exemption vendors of mobile computing devices are likely to claim that when users circumvent technological protection measures, they violate manufacturers' copyrights in the device firmware. The shadow of legal liability from § 1201 will discourage users from engaging in legitimate, non-infringing modification of their devices, and thus hinder the numerous innovators who might otherwise find a market for their applications.[20]

Jailbreaking remains an important and lawful activity, but for the prohibition on circumvention. We ask the Librarian to renew and expand the exemption for jailbreaking.

---

[16] *Id.*; *Perfect 10*, 508 F.3d at 1167; *Sony*, 203 F.3d at 605-06.
[17] 2012 Recommendation at 73.
[18] *Campbell*, 510 U.S. at 590.
[19] 2010 Recommendation at 103; *see also* 2012 Recommendation at 74-75.
[20] *See, e.g.,* Responsive Comment of Apple Inc. In Opposition to Proposed Exemption 5A and 11A (Class #1) at 11-13, http://www.copyright.gov/1201/2008/responses/apple-inc-31.pdf.