

Abstract

This Article reviews the creation of the Apple iPhone and the function of technological protection measures that are put in place by Apple for various control purposes. It also reviews the process of “unlocking” and “jailbreaking” an iPhone and the legality that rests on this hacking technique.

Section one will explain the process of “unlocking” and “jailbreaking” an iPhone, what purpose is served by performing these processes, and the interests of Apple in preventing jailbreaking including a review of the protective measures that have been put in place by Apple to prevent the jailbreaking from happening.

Section two will outline the law surrounding the processes of unlocking and jailbreaking. This will include an overview of The Digital Millennium Copyright Act § 1201(a)(1) which specifically prohibits the circumvention of protection measures like the ones put in place on the iPhone by Apple.

Section three details the current litigation brought by the Electronic Frontier Foundation (“EFF”) and Apple where the EFF petitioned the Librarian of Congress to make an exemption for jailbreaking and Apple, in response to the EFF’s petition, wrote its own petition to the Librarian of Congress.

Finally, section four will explain why the Librarian of Congress should allow an exemption for jailbreaking an iPhone for lawful purposes. Not only is it in conjunction with the current Exemption Five, but jailbreaking causes more benefit to Apple than harm, and those who violate copyright law by providing “cracked” Apple applications to the public can still be found liable under the law.

Table of Contents

INTRODUCTION	Page 1
THE IPHONE	Page 2
<i>A. Unlocking</i>	Page 3
<i>B. Jailbreaking</i>	Page 4
<i>C. Technological Protection Measures</i>	Page 6
ARE UNLOCKING AND JAILBREAKING ILLEGAL?	Page 9
<i>A. Digital Millennium Copyright Act: 1201(a)(1)</i>	Page 9
<i>B. Exemption Five</i>	Page 13
<i>C. The Legality of Jailbreaking After October 27, 2009</i>	Page 15
INTERESTED PARTIES & LITIGATION	Page 16
PROPOSED REASONS FOR EXEMPTING JAILBREAKING FROM § 1201	Page 21
CONCLUSION	Page 25

Jailbreaking and Unlocking the iPhone: The legal implications

INTRODUCTION

This Article reviews the creation of the Apple iPhone and the function of technological protection measures that are put in place by Apple for various control purposes. Section one explains the process of “unlocking” and “jailbreaking” an iPhone, what purpose is served by performing these processes, and the interests of Apple in preventing jailbreaking including a review of the protective measures that have been put in place by Apple to prevent the jailbreaking from happening.

Section two will outline the law surrounding the processes of unlocking and jailbreaking. The Digital Millennium Copyright Act § 1201(a)(1) specifically prohibits the circumvention of protection measures like the ones put in place on the iPhone by Apple. However, § 1201(f) provides an exception for the circumvention of protection measures when done through reverse engineering to increase the interoperability of the device. Jailbreaking is a form of reverse engineering, but as explained *infra*, the licensing of Apple’s iPhone operating system does not allow for reverse engineering. Under § 1201, the Librarian of Congress shall hold a rulemaking every three years to provide exemptions to § 1201. Currently Exemption Five allows for the unlocking of a cell phone to connect lawfully to any wireless network, but jailbreaking is not covered by any current exemption. The new ruling for 2009 was set to take effect October 27, 2009 but has been postponed with an interim ruling extending the most recent exemptions until a final ruling is made.

Section three details the current litigation brought by the Electronic Frontier

Foundation (“EFF”) and Apple. The EFF has petitioned the Librarian of Congress to make an exemption for jailbreaking and explains its purpose through several compelling reasons. Apple, in response to the EFF’s goal, wrote its own petition to the Librarian of Congress and has too listed compelling reasons for its objective in not allowing an exemption to be made for circumventing its technological protection measures.

Finally, section four will explain why the Librarian of Congress should allow an exemption for jailbreaking an iPhone for lawful purposes. Not only is it in conjunction with the current Exemption Five, but jailbreaking causes more benefit to Apple than harm, and those who violate copyright law by providing “cracked” Apple applications to the public can still be found liable under the law.

1. THE IPHONE

It was June 29, 2007 when Apple released its long-awaited iPhone, “a product hailed as revolutionary, unprecedented, and more advanced than any other mobile or ‘smart’ phone...in the marketplace.”¹ The device was an all-in-one Internet browser, music player, digital personal assistant, and telephone.² What made this smart phone stand out from similar phones was that its web browser was fully functional, its voicemail was visual, its music player was an iPod, the email was desktop-class, and it included a built-in accelerometer (useful for iPhone application developers).³ To top it all of,

¹ David L. Hayes, *Responsive Comment of Apple Inc. In Opposition to Proposed Exemption 5A and 11A (Class #1)* at 3 (2008), <http://www.copyright.gov/1201/2008/responses/apple-inc-31.pdf>.

² Matthew Yoeli, Apple’s iPhone: the Case for Broadening Exemption Five to 17 U.S.C. § 1201 to Ensure Continued Non-Infringing Use of Wireless Communication Handsets, 37 *AIPLA QUARTERLY J.* 83, 85-86 (2009).

³ Hayes, *supra* note 1 at 3-4.

everything was provided through a “groundbreaking Multi-Touch™ user interface.”⁴ It took Apple only 74 days to sell over one million iPhones making it “one of the most successful product introductions in the history of cellular telephony.”⁵ Not only did the iPhone set sales records but it established a new demand for what consumers want in a mobile communication device.

A. Unlocking

Although sold initially to the United States alone, the iPhone has now been made available to over eighty countries.⁶ In some countries, Apple has an exclusive partnership with a wireless carrier to provide the data and voice service for the iPhone.⁷ In conjunction with these agreements, Apple built a locking mechanism into the iPhone's firmware; this firmware has the capacity to limit the iPhone to the single wireless network with which Apple has agreed to be exclusive.⁸ This is achieved by designing the phone to operate using a Subscriber Identification Module (“SIM”) card—a microchip that keeps the subscriber's data.⁹ The SIM technology is common among cell phones.¹⁰ A “locked” phone only recognizes a SIM card subscribed to a specific carrier.¹¹ But, if one

⁴ *Id.*

⁵ *Id.* at 3 citing “Apple Sells One Millionth iPhone” (Press Release, Apple Inc., Jan. 9, 2007), available at www.Apple.com/pr/library/2007/09/10iphone.html.

⁶ Yoeli, *supra* note 2 at 86.

⁷ *Id.*

⁸ *Id.* at 87.

⁹ WiseGeek.com, What is a Sim Card?, <http://www.wisegeek.com/what-is-a-sim-card.htm> (last visited Mar. 5, 2010).

¹⁰ WiseGeek.com, What Are Unlocked Cell Phones, <http://www.wisegeek.com/what-are-unlocked-cell-phones.htm> (last visited Mar. 5, 2010).

¹¹ *Id.*

“unlocks” the cell phone¹², it will recognize a SIM card from any carrier.¹³ The “lock” is a software program that makes the cell phone loyal to a single carrier.¹⁴

If this firmware locking mechanism was not in place, then the iPhone could connect to any wireless network that operated under the Global System for Mobile communications standard (“GSM”)—the network that is used by approximately eighty-six percent of the world-wide cellular market.¹⁵ This is desirable for many consumers who are under contract with a different wireless carrier but want to use an iPhone for his or her cellular device.

Currently there are several software programs that unlock the iPhone by rendering its firmware lock inoperative.¹⁶ Utilizing any of these software programs for the iPhone, as explained above, allows the device to be open to use on any GSM network.¹⁷ In the United State’s, AT&T responded to these unlocking efforts by threatening legal action against the creators of unlocking software if they release the unlock code,¹⁸ and Apple began to release updates for the iPhone software that reinstated the firmware lock.¹⁹ In the events to follow, consumers were outraged by Apple’s steps taken to protect a contract with its wireless carrier, and moreover, rage came from consumers whose locked iPhones were left forever inoperable by the firmware updates and Apple’s refusal to

¹² See Dev-Team Blog, <http://blog.iphone-dev.org/>, http://www.pcworld.com/article/137223/how_to_unlock_an_iphone.html (last visited Mar. 5, 2010) (information and how-tos for unlocking an iPhone).

¹³ WiseGeek.com, *supra* note 10.

¹⁴ *Id.*

¹⁵ Yoeli, *supra* note 2 at 87-88.

¹⁶ *Id.* 2 at 88.

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ *Id.*

repair these now inoperable phones under its warranty.²⁰

B. Jailbreaking

The firmware lock not only furthers Apple's efforts to impose its exclusive wireless carrier agreements,²¹ it also allows Apple to profit off of the creation of third-party software for the iPhone. When the iPhone first came out, a user could use and access web applications, but not use the device in conjunction with any application that a consumer could download from a third party.²² For security and functionality purposes, “Apple briefly delayed support for third party applications.”²³ “This decision did not dampen overall consumer enthusiasm for the product, and Apple continued to develop and refine the iPhone technology and maintain and improve its security, reliability and overall functionality.”²⁴ After Apple successfully launched the iPhone, it finally turned to applications made by third parties; Apple used an approach to foster the development of third-party applications that has been deemed revolutionary.²⁵ Since the firmware lock limits the use of the iPhone's bootloader (the mechanism that allows software programs to be loaded into memory) to load only software that Apple has approved, it seems that Apple wants to maintain its profit interest by restricting the bootloader from loading programs that Apple has not approved.²⁶ Without this level of access to the iPhone through the bootloader, consumers cannot load programs or customize audiovisual

²⁰ *Id.*

²¹ Yoeli, *supra* note 2 at 88.

²² Hayes, *supra* note 1 at 4.

²³ *Id.*

²⁴ *Id.*

²⁵ *Id.* citing Marguerite Reardon, “Apple answers call for iPhone applications,” *cNet.com*, June 10, 2008, available at http://www.news.cnet.com/8301-10784_3-9964401-7.html.

²⁶ Yoeli, *supra* note 2 at 89.

settings.²⁷

Again, like the consumers who wanted to utilize the iPhone on a network other than AT&T, there were consumers who also wanted to use programs that were not available through the Apple App Store. Many reasons, ranging from innocent to illegal, exist for wanting to access unauthorized third-party applications. For instance, Apple has yet to release an application for the iPhone that will allow the consumer to change the “theme.” One who buys an iPhone is restricted to icons and colors that are already on the phone, leaving only the customization of ring tones and the locked screen background for the consumer to adjust. For the creative minds, jailbreaking one’s iPhone is desirable in that a jailbroken phone can utilize third-party application not available through the App Store such as the program Winterboard. Winterboard, among other third-party programs, allows the consumer to adjust everything from icons and unlocked screen background, to loading a pre-made “theme” to the phone that will adjust almost everything about the look of the phone.²⁸ However, jailbreaking is also desirable for illegal purposes. One who possesses a jailbroken phone can access and install actual App Store applications that have had their protection measures overridden without paying for the copyrighted program.²⁹ This can be done manually or by downloading the already cracked apps from

²⁷ *Id.*

²⁸ See iPhone Heat, Winterboard | How to Customize your iPhone with WinterBoard | Winterboard Features | iPhoneHeat, <http://www.iphoneheat.com/2009/04/how-to-customize-your-iphone-with-winterboard-step-by-step-guide/> (last visited Mar. 5, 2010).

²⁹ See Appylo.us, Appulo.us :: Moving On, <http://appulo.us/appdb/> (last visited Mar. 5, 2010) (this website is no longer providing these services), See Also Apptrackr – The Source for iPhone Apps <http://apptrackr.org/> (last visited Mar. 5, 2010) (this website is no longer providing these services).

websites like Appulous³⁰ and Apptrackr³¹.

C. Technological Protection Measures

Technological protection measures are what must be overridden in order to accomplish either unlocking or jailbreaking an iPhone. Apple has established these technological protection measures for a number of reasons, one being to retain control of the distribution of iPhone applications.³² The purpose as stated by Apple, is to protect the consumer from installing things such as malware on the iPhone, thus preventing costs for Apple in repairs and replacements of phones.³³ Apple attempted to achieve this purpose by creating the App Store, a one-stop-shop for iPhone applications.³⁴ The App Store development process began March 2008 when Apple established the new iPhone Developer Program.³⁵ This included the release of Apple's iPhone Software Development Kit required to create programs for the iPhone to registered developers who have initially paid a fee.³⁶ The software development kit contained "a rich and powerful set of application programming interfaces (APIs) and tools enabling independent software developers to design applications for the iPhone."³⁷ Over 100,000 copies of the SDK were downloaded "within the first four days after its launch."³⁸ This "ballooned to

³⁰ Appulo.us, Appulo.us :: Moving On, <http://appulo.us/appdb/> (last visited Mar. 5, 2010) (this website is no longer providing these services).

³¹ Apptrackr – The Source for iPhone Apps <http://apptrackr.org/> (last visited Mar. 5, 2010) (this website is no longer providing these services).

³² Hayes, *supra* note 1 at 9.

³³ *Id.* at 8.

³⁴ *Id.* 9.

³⁵ *Id.* 4.

³⁶ Yoeli, *supra* note 2 at 89.

³⁷ Hayes, *supra* note 1 at 4 citing "Apple Announces iPhone 2.0 Software Beta" (Press Release, Apple Inc., March 6, 2008), available at <http://www.apple.com/pr/library/2008/03/06iphone.html>.

³⁸ Hayes, *supra* note 1 at 4.

250,000 in a little over three months as iPhone application developers proliferated.”³⁹

Apple also requires that all iPhone software be circulated exclusively through its App Store where Apple collects thirty percent of the sales revenue.⁴⁰

Apple later “released its second-generation 3G iPhone and version 2.0 of the iPhone operating software” in July 2008, “which was designed to allow iPhone owners to safely and reliably download third party applications.”⁴¹ Also at this time, “Apple opened its groundbreaking iPhone App Store—a centralized repository where developers post, and users seamlessly review, preview and download thousands of newly created third party applications.”⁴² “In the first weekend after opening, the App Store saw 10 million application downloads.”⁴³ “In just seven months since it was launched, the App Store [contained] over 15,000 applications, and consumers [had] made over 500 million downloads.”⁴⁴

“Apple engineers have designed the iPhone to contain technological protection measures...that protect two critical pieces of software resident in the device that are core to its functioning – the bootloader and the operating system (“OS”).”⁴⁵ The bootloader is

³⁹ Hayes, *supra* note 1 at 4 citing “iPhone SDK Downloads Top 100,000” (Press Release, Apple Inc., March 12, 2008), available at <http://www.apple.com/pr/library/2008/03/12iphone.html>; “iPhone SDK Downloads Top 250,000” (Press Release, Apple Inc., June 9, 2008), available at http://www.apple.com/pr/library/2008/06/09iphone_sdk.html.

⁴⁰ Yoeli, *supra* note 2 at 89.

⁴¹ Hayes, *supra* note 1 at 5.

⁴² *Id.*

⁴³ *Id.* citing “iPhone App Store Downloads Top 10 Million in First Weekend” (Press Release, Apple Inc., July 14, 2008), available at <http://www.apple.com/pr/library/2008/7/14appstore.html>.

⁴⁴ Hayes, *supra* note 1 at 5 citing Jefferson Graham, “Application developers see iPhone as way to get noticed,” *USE Today*, January 20, 2009, available at http://www.usatoday.com/tech/products/services/2009-01-20-phanfare-Internet-photos-iphone_N.htm.

⁴⁵ Hayes, *supra* note 1 at 7, citing the iPhone Software License Agreement that governs the use of the software on the iPhone, the bootloader is referred to as the “Boot ROM code.” Apple iPhone Software License Agreement, §1, available at <<http://images.apple.com/legal/sla/docs/iphone.pdf>>.

a small computer program that runs automatically when the phone is turned on.⁴⁶ It runs initial hardware tests and then loads the OS onto the main memory for operation.⁴⁷ The OS functions as the “core operating software” for the device.⁴⁸ The OS handles the operation details of the hardware, and manages and coordinates the activities and operations necessary for making and receiving phone calls, “and for application programs (such as email and calendar) to execute on the device.”⁴⁹ Apple has copyright ownership of the bootloader and the OS.⁵⁰

The OS, as the iPhone’s key operational component, offers functions or services that applications can access through the application programming interfaces.⁵¹ By using these application programming interfaces and system calls, an application program can request a service from the OS (such as reading or writing data), pass parameters, and receive the results of an operation.⁵² Another option for the user to interact with the OS is through the phone’s graphical user interface; this is generally considered a part of the OS itself.⁵³ The iPhone “was designed not just to enable the making of phone calls, but specifically to provide a rich mobile computing platform so that Apple, applications developers and iPhone users could all benefit from a very wide range of functionality.”⁵⁴ Apple insisted in their submission to the U.S. Copyright Office regarding the EFF’s request for an exemption for the prohibition on circumvention of access controls, that

⁴⁶ Hayes, *supra* note 1 at 7.

⁴⁷ *Id.*

⁴⁸ *Id.*

⁴⁹ *Id.*

⁵⁰ *Id.*

⁵¹ *Id.*

⁵² Hayes, *supra* note 1 at 7.

⁵³ *Id.* at 7-8.

⁵⁴ *Id.* at 8.

the significance of the iPhone OS to Apple's entry and long-term product strategy cannot be overstated. The platform provided by the OS has created positive feedback loops so that a large community of developers [have] been willing to invest in iPhone technologies, elevate the platform and the iPhone user experience, and benefit themselves, Apple and consumers alike.⁵⁵

The iPhone contains several Technological Protection Measures that “protect the bootloader and OS from modification or corruption, and verify their origin, thereby helping to ensure proper functioning of the device.”⁵⁶ The hardware's read only memory (“ROM”) “contains cryptographic keys that are used to validate the bootloader and the OS.” When the device is turned on, “the secure ROM uses the keys to validate the bootloader before loading it (by verifying its digital signature), and the bootloader then validates the OS before loading it for execution (again, by verifying its digital signature).” The process establishes “that the bootloader and OS originated from Apple and that they have not been altered.”⁵⁷ When version 2.0 of the OS came out, the OS also validated “all application programs loaded into the iPhone [by] their digital signatures to confirm that they have been accepted by Apple for execution on the iPhone and have not been altered.”⁵⁸ Apple refers to this sequence as the “*chain of trust*.”⁵⁹

The iPhone's Technological Protection Measures prevent applications from running that are not obtained through Apple's iTunes App Store.⁶⁰ A 30% commission fee must be paid to Apple by the Independent software developers if they want to sell

⁵⁵ *Id.*

⁵⁶ *Id.*

⁵⁷ *Id.*

⁵⁸ Hayes, *supra* note 1 at 8.

⁵⁹ *Id.*

⁶⁰ Fred von Lohmann, *Comments of the Electronic Frontier Foundation in Support of Proposed Classes 5A, 5D, 11A and of The Wireless Alliance, ReCellular and FlipSwap in Support of Proposed Class 5D* at 5 (2008), <http://www.copyright.gov/1201/2008/responses/electronic-frontier-foundation-50.pdf>.

software through Apple's App Store.⁶¹ Despite Apple's stringent regulations, many iPhone applications created by third parties, as mentioned above, are available to the iPhone owners who have "jailbroken" their iPhones.

2. ARE UNLOCKING AND JAILBREAKING ILLEGAL?

A. Digital Millennium Copyright Act: 1201(a)(1)

Though wireless devices commonly use firmware locks,⁶² their legality under United States law remains disputed.⁶³ The dispute is focused on the phrasing of the Digital Millennium Copyright Act ("DMCA").⁶⁴ The DMCA serves as a needed amendment to the Copyright Act of 1976⁶⁵ in an effort to bring the law "squarely into the digital age."⁶⁶ Two international treaties signed in front of the World Intellectual Property Organization ("WIPO") are codified by the DMCA, and it establishes novel provisions that tackle the reliability of copyright management information.⁶⁷

The DMCA, codified in part at 17 U.S.C. § 1201 (2006) ("Section 1201"), guards copyright management information by barring the circumvention of technological measures that restrict access to copyrighted works.⁶⁸ According to section 1201, three types of anti-circumvention violations exist: "a basic provision, a ban on trafficking, and

⁶¹ *Id.*

⁶² Yoeli, *supra* note 2 at 90.

⁶³ *Id.*

⁶⁴ *Id.*

⁶⁵ *Id.*

⁶⁶ *Id.*

⁶⁷ *Id.*

⁶⁸ Yoeli, *supra* note 2 at 91.

‘additional violations.’”⁶⁹ The broad scope of the Basic Prohibition by section 1201 is limited, however, by allowing certain uses of copyrighted works pursuant to a rulemaking proceeding.⁷⁰ The intent behind this rulemaking proceeding is to have a “fail-safe” mechanism in place to protect lawful access to copyrighted works if they ever become unduly restricted.⁷¹ To carry out this procedure, the Librarian of Congress, upon the recommendation of the Register of Copyrights, determines and publishes three-year exemptions for non-infringing uses of copyrighted works that are adversely affected, or likely to be adversely affected, by the Basic Prohibition.⁷² In determining this, the statute necessitates the Librarian of Congress to review the five factors listed in Section 1201(a)(1)(C); these include the copyrighted work's availability for use, the impression of the Basic Prohibition on the market value or for of the copyrighted work, and other suitable factors.⁷³

The DMCA’s legislative history shows that the legislature was concerned with the consequences of Section 1201 on the copyright’s longstanding principle of “fair use.”⁷⁴ This principle, which was eventually codified in 17 U.S.C. § 107...states that “he fair use of a copyrighted work ... is not an infringement of copyright.”⁷⁵ A fair use determination requires a balancing test that “takes into account the interests of copyright owners and the competing needs of those who use and rely upon copyrighted materials and

⁶⁹ *Id.*

⁷⁰ *Id.*

⁷¹ *Id.*

⁷² *Id.*

⁷³ *Id.* at 92.

⁷⁴ Yoeli, *supra* note 2 at 92.

⁷⁵ *Id.*

information.”⁷⁶ Several factors are listed for determination of whether a use is “fair.” These factors include “the purpose and character of the use, the nature of the copyrighted work, and the effect of the use on the market for, or value of, the copyrighted work.”⁷⁷ “These factors are markedly similar to those that the Librarian of Congress uses in determining exemptions to Section 1201,⁷⁸ which demonstrates that fair use was a motivating factor in the creation of the exemption rulemaking process.”⁷⁹ This is further shown by the Librarian of Congress’s description of fair use as a “possible non-infringing use of a copyrighted work.”⁸⁰

Section 1201(f) is an exception found in the DMCA to circumventing protection measures done through reverse engineering “for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention.”⁸¹ Section 1201(f) on its face seems to encompass jailbreaking since the sole purpose of jailbreaking is to make the phone interoperable with other applications. However, the scant amount of case law on the issue provides a much narrower interpretation of § 1201(f).

*Universal City Studios v. Reimerdes*⁸² was the first and only case to

⁷⁶ *Id.*

⁷⁷ *Id.*

⁷⁸ *Id.*

⁷⁹ Yoeli, *supra* note 2 at 93.

⁸⁰ *Id.*

⁸¹ The Digital Millennium Copyright Act, 17 U.S.C. § 1201(f) (1998).

⁸² *Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 2d 211 (S.D.N.Y. 2000).

consider § 1201(f).⁸³ In this case, plaintiff claimed that defendant distributed DeCSS, a program that overrode the Content Scramble System (“CSS”), which prevented the decryption of DVDs.⁸⁴ The defendants claimed that DeCSS was protected under § 1201(f) since it allowed DVDs to interoperate the Linux operating system.⁸⁵ The court in *Reimerdes* provided a narrow interpretation of § 1201(f) limiting it to circumvention of protection measures in computer programs and not copyrighted works in general.⁸⁶ This left the defendants defenseless since CSS restricted access to movies rather than computer programs.⁸⁷ The narrow interpretation additionally heightened the sole purpose requirement of § 1201(f) so that reverse engineering may only be done for the “sole purpose” of achieving interoperability.”⁸⁸

After *Reimerdes*, § 1201(f) has undertaken little judicial analysis.⁸⁹ Not one defendant, in the few published opinions, has successfully raised a § 1201(f) defense.⁹⁰ Further interpretation of § 1201 has been provided however through a one notable case. In *Chamberlain Group v. Skylink*⁹¹ the court held that to “maintain an action under § 1201, a plaintiff must establish not only that an effective TPM restricts access to a copyrighted work, but that the circumvention

⁸³ Aaron K. Perzanowski, *Rethinking Anticircumvention’s Interoperability Policy*, 42 U.C. DAVIS LAW REVIEW 1549, 1574 (2009).

⁸⁴ *Id.*

⁸⁵ *Id.*

⁸⁶ *Id.* at 1574-75.

⁸⁷ *Id.* at 1575.

⁸⁸ Perzanowski, *supra* note 83 at 1575.

⁸⁹ *Id.* at 1577.

⁹⁰ *Id.*

⁹¹ *Chamberlain Group, Inc. v. Skylink Tech., Inc.*, 381 F.3d 1178 (Fed. Cir. 2004).

of that TPM bears some ‘reasonable relationship to the protections that the Copyright Act otherwise affords.’”⁹² Unfortunately the *Chamberlain* court did not analyze § 1201(f).

One year after *Chamberlain*, the Eighth Circuit Court of Appeals provided the most stringent analysis of § 1201(f) to date.⁹³ *Davidson & Associates v. Jung*⁹⁴ found that “[t]he statute...only exempts those who obtained permission to circumvent the technological measure.”⁹⁵ This holding is flawed in that it undermines the purpose of having an exemption in the first place. This absurd logic, if applied to copyright law in general, could eliminate the law of fair use completely. These exemptions have a purpose—to provide narrow defenses to those who fail to obtain permission from copyright owners. Jailbreaking is not reached by § 1201(f) as interpreted by case law. Consumers who have jailbroken their phone are not likely to have Apple grant permission to jailbreak because it violates their licensing agreement, which specifically prohibits reverse engineering.⁹⁶

B. Exemption Five

Six exemptions to Section 1201 were published on November 27, 2006 by The Librarian of Congress to be in effect through October 27, 2009.⁹⁷ A document was printed to announce these exemptions (“LOC Notice”), which put forth the reasons for

⁹² *Perzanowski*, *supra* note 83 at 1578.

⁹³ *Id.* at 1585.

⁹⁴ *Davidson & Assocs. v. Jung*, 422 F.3d 630 (8th Cir. 2005).

⁹⁵ *Id.* at 640-42.

⁹⁶ Apple.com, Apple – Legal – iPhone Warranty – Original, iPhone Warranties, <http://www.apple.com/legal/warranty/iphone/original.html>.

⁹⁷ Yoeli, *supra* note 2 at 93.

each exemption and what was necessary to make a prima facie case for each exemption.⁹⁸

The exemption applicable to the iPhone's current situation is the fifth exemption ("Exemption Five"). Exemption five applies to "[c]omputer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network."⁹⁹ The LOC Notice accorded that Exemption Five was issued "in order to give consumers the opportunity to make lawful use of the software on their cellular phones."¹⁰⁰ Numerous wireless service providers load firmware locks on the phones that are sold in order to limit the phones to its network.¹⁰¹ Without firmware unlocking capabilities, consumers cannot use their phones on competing networks—even post-contract.¹⁰² This inconvenience led to the Librarian of Congress's conclusion that this Section 1201 exemption was compelling since firmware locks "adversely affect the ability of consumers to connect lawfully to any wireless carrier."¹⁰³

The LOC Notice also explained how Exemption Five is in harmony with the five factors enumerated in Section 1201(a)(1)(C).¹⁰⁴ Highlighted specifically was that wireless cell phone firmware locks restrict the ability of the cellular subscribers to change their service lawfully to a wireless carrier competitor, "a business decision unrelated to

⁹⁸ Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. at 68,472-79 (2009).

⁹⁹ 37 C.F.R. § 201.40(b)(5).

¹⁰⁰ Yoeli, *supra* note 2 at 94 (citing *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. at 68,476).

¹⁰¹ Yoeli, *supra* note 2 at 94.

¹⁰² *Id.* at 95.

¹⁰³ *Id.*

¹⁰⁴ *Id.*

the interests protected by copyright.”¹⁰⁵ The Librarian of Congress thus concluded that Exemption Five should be customized only to permit the circumvention of firmware locks for the purpose of lawfully connecting to a wireless network.¹⁰⁶

The Librarian of Congress drastically narrowed the black letter of the exemption as originally proposed which allowed the circumvention of “[c]omputer programs that operate wireless communication handsets.”¹⁰⁷ The Librarian of Congress has concluded that Exemption Five should be customized only to permit the circumvention of firmware locks for the purpose of lawfully connecting to a wireless network.¹⁰⁸ Unlocking an iPhone so that one may lawfully connect to another network other than AT&T is permitted under the law; however, jailbreaking is different from unlocking in that unlocking is the removal of SIM restricts on the modem, and jailbreaking is the modification of iPhone firmware to allow unsigned code to be run to gain access to files that Apple would not normally let you access; so jailbreaking does not fall within the exemption as interpreted by the Librarian of Congress.¹⁰⁹

C. The Legality of Jailbreaking After October 27, 2009

The six exemptions published on November 27, 2006 expired October 27, 2009 and have been up for review by the Librarian of Congress, along with other proposals for exemption.¹¹⁰ The Register of Copyrights is currently conducting the fourth of these

¹⁰⁵ *Id.*

¹⁰⁶ *Id.* at 96.

¹⁰⁷ Yoeli, *supra* note 2 at 96.

¹⁰⁸ *Id.*

¹⁰⁹ The Difference Between Jailbreaking and Unlocking, <http://www.iphonedownloadblog.com/2009/07/10/difference-jailbreaking-unlocking/> (last visited Mar. 5, 2010).

¹¹⁰ Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control

triennial rulemaking proceedings and is still in the final stages of making a recommendation to the Librarian of Congress, so an interim rule has been made for the time being.¹¹¹ Because the Register was not able to present her recommendation to the Librarian of Congress before October 27, the Register stated it was “necessary to extend the effective dates of the existing regulation identifying those classes of works until the time that the Librarian acts upon the recommendation of the Register.”¹¹² The Register anticipates that the extension will be in effect for no more than a few weeks.¹¹³

However, there has not been an updated action to date. The Librarian of Congress accepted the recommendation of the Register of Copyrights and adopted the interim rule.

114

3. INTERESTED PARTIES & LITIGATION

Because there is a desire by many consumers to have an unlocked or jailbroken iPhone, legal debate has ensued regarding the legality of unlocking and jailbreaking one’s iPhone. Compelling arguments have been made on both sides. This article will focus on the arguments made by Apple and the Electronic Frontier Foundation—an organization that has been deeply involved in the U.S. Copyright Office’s 2009 rulemaking on the issues surrounding the legality of both unlocking and jailbreaking).

Technologies 71 Fed. Reg. 227 at 2-6 (Nov. 27, 2006)
<http://www.copyright.gov/fedreg/2006/71fr68472.pdf>.

¹¹¹ Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies 74 Fed. Reg. 206 <http://www.copyright.gov/fedreg/2009/74fr55138.pdf>.

¹¹² *Id.*

¹¹³ *Id.*

¹¹⁴ *Id.*

The 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.”¹¹⁵ The organization was founded in 1990 and represents over 13,000 due-paying members including hobbyists, consumers, entrepreneurs, computer programmers, researchers, students, and teachers—all united in their fight for a balanced copyright system that guarantees copyright owners’ adequate protection while maintaining broad access to information in the digital age.¹¹⁶ Through these practices, the EFF embodies the “interest of hundreds of thousands of citizens who have ‘jailbroken’ their [cell phones]...in order to use lawfully obtained software of their own choosing.”¹¹⁷

The EFF submitted a comment to the Librarian of Congress requesting that “[c]omputer programs that enable wireless telephone handsets to execute lawfully obtained software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications with computer programs on the telephone handset” be exempt from 17 U.S.C. § 1201(a)(1)’s prohibition on the circumvention of access control technologies for the period of 2009 through 2012.¹¹⁸ More clearly, the EFF proposes that “jailbreaking” falls under § 1201(f), an already enumerated exception to circumventing protection measures done through reverse engineering “for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created

¹¹⁵ Lohmann, *supra* note 60 at 1.

¹¹⁶ *Id.*

¹¹⁷ *Id.* at 2.

¹¹⁸ *Id.* at 1.

computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention.”¹¹⁹

The EFF began their submission by explaining their idea of the proper role of fair use and other limitations and exceptions in this type of proceeding. The EFF urged the Librarian to adopt a modern approach when assessing fair use and the other statutory exceptions that should be taken into account.¹²⁰ The approach was summarized as follows:

[W]here assertions of fair use or other statutory exceptions lead the Librarian into areas that have not yet been addressed by the courts, the Librarian should err on the side of accepting these assertions of noninfringement, but narrow any resulting exemption to activities that are ultimately found by the courts to be noninfringing.¹²¹

The EFF argued that “Congress intended the DMCA's triennial rulemaking to act as a ‘fail-safe mechanism’ to mitigate the risk that access controls on copyrighted works would interfere with otherwise lawful uses of those works.”¹²² Accordingly, the EFF pointed out that the “Copyright Office has noted, ‘[t]he goal of the proceeding is to assess whether the implementation of technological protection measures that effectively control access to copyrighted works is adversely affecting the ability of individual users to make lawful uses of copyrighted works.’”¹²³ Strategically the EFF listed fair use as one of the lawful uses Congress intended to preserve when enacting § 1201, and thus preserving fair use in this context of rulemaking poses a challenge: “how can the courts continue to develop fair use jurisprudence in light of new technologies and practices if the activities

¹¹⁹ The Digital Millennium Copyright Act, 17 U.S.C. §1201(f) (1998).

¹²⁰ Lohmann, *supra* note 60 at 2.

¹²¹ *Id.*

¹²² *Id.*

¹²³ *Id.*

in question are impeded by access controls?”¹²⁴

The EFF, as proponents of an exemption, bore the burden of proving that their intended use was not an infringing one.¹²⁵ The EFF believed that in cases that “fall comfortably within the ambit of settled fair use precedents,”¹²⁶ “it is a simple matter for the Librarian to recognize the noninfringing nature of the activity and move on to weigh the other factors that must be considered in evaluating a proposed exemption.”¹²⁷ However, not all fair-use questions are so clear.¹²⁸ “Because Congress has left fair use for the courts to develop on a case-by-case basis, there are always many activities on which the courts have not yet passed.”¹²⁹ Fair Use’s ability to evolve “in light of new technologies and practices” was stated as “one of its great strengths” according to the EFF.¹³⁰ However, The EFF said that this unfortunately posed a dilemma.¹³¹ It was provided that only if the proceeding granted exemptions in “untested cases” would the courts “have an opportunity to address fair-use claims involving new technologies and practices.”¹³² The EFF urged that “[d]enying exemptions based on the Librarian’s best guesses about how a court might rule on these questions... would potentially set the Librarian up as the final arbiter of statutory exceptions

¹²⁴ *Id.*

¹²⁵ *Id.*

¹²⁶ Lohmann, *supra* note 60 at 2.

¹²⁷ *Id.*

¹²⁸ *Id.*

¹²⁹ *Id.* at 2-3.

¹³⁰ *Id.* at 3.

¹³¹ Lohmann, *supra* note 60 at 3.

¹³² *Id.*

with regard to works subject to access controls.”¹³³

To resolve this dilemma, the EFF proposed “the Librarian adopt the following approach when evaluating an assertion of fair use or other statutory exception:”

If, based on existing precedents, the Librarian is satisfied that the activity in question is likely to be deemed to be a fair use or otherwise covered by a statutory exception, then the Librarian should conclude that the activity is noninfringing and proceed to weigh the other factors that must be considered in evaluating a proposed exemption; 2. If the Librarian is satisfied that the activity in question might plausibly be a fair use or be protected by any other statutory exception, but has some doubt on the question, then the Librarian should narrow the proposed exemption to apply only so long as the activity in question is noninfringing; 3. If the Librarian concludes that no reasonable court could find that the activity in question would constitute a fair use or fall within any other statutory exception, it should reject the proposed exemption.¹³⁴

The EFF believed that its approach comported “with both the letter and spirit of this rulemaking.”¹³⁵ Under the EFF’s approach,

[w]here a proposed exemption turns on the application of fair use or another statutory exception in a context that has not been definitively addressed by the courts, this approach would favor granting the exemption...thereby allowing circumventers to bring their fair use or other statutory defenses to the courts for resolution.¹³⁶

They said that this would in turn “foster the development of judicial precedents that will assist the Librarian in future rulemaking proceedings.”¹³⁷ They pointed out that “[a]t the same time, an exemption whose scope is limited only to activities that are

¹³³ *Id.*

¹³⁴ *Id.* at 3-4.

¹³⁵ *Id.* at 4.

¹³⁶ Lohmann, *supra* note 60 at 4.

¹³⁷ *Id.*

noninfringing does not release any infringers.”¹³⁸ So “[i]f litigation were to ensue, the defendant would be entitled to mount her defense to the claim of infringement” and “a successful defense on the question of infringement would thus also result in a successful defense to any circumvention claim.”¹³⁹ “In contrast, a failed fair use defense and finding of infringement would simultaneously disqualify the defendant from relying on the exemption as a shield against circumvention liability.”¹⁴⁰ The EFF said that “[t]his ‘double jeopardy’ should preserve any deterrence value that the ban on circumvention would otherwise provide.”¹⁴¹

The EFF urged that “[i]f the courts are to continue to develop the jurisprudence of fair use and other statutory exceptions notwithstanding the increasing use of access controls on copyrighted works, the triennial rulemaking must allow as-yet untested questions to find their way to the courts.”¹⁴² They believe their approach “strikes this balance, preserving for the courts their traditional role as case-by-case adjudicators of fair use and other statutory exceptions.”¹⁴³

In its submission to the U.S. Copyright Office—coexisting as a response to the EFF’s proposal for allowing circumvention of iPhone’s technological protection measures—Apple listed three overarching reasons for protecting its OS through these TPMs:

- (1) The OS implements a number of essential safety and control functions. For example, it monitors the thermal condition of the device and shuts it

¹³⁸ *Id.*

¹³⁹ *Id.*

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

¹⁴² Lohmann, *supra* note 60 at 4.

¹⁴³ *Id.*

down if it is overheating. It controls the charging of the battery, instructing the relevant circuitry when to start and stop charging the battery, and at what level to charge it. The OS also implements certain governors on the phone's volume. If modifications to the OS were to interfere with these control functions, even unintentionally, the phone could be physically damaged or the battery could be overcharged.

(2) The OS implements a number of security functions that protect both the iPhone itself and the telephone network to which it connects. For example, the OS implements certain controls on how application programs are able to execute on the iPhone to help prevent viruses and other forms of "malware" from executing. Modification of the OS can interfere with these functions and open up security holes that could enable malware to accomplish malicious things through the iPhone, such as stealing information from the user's contacts database. The OS also controls a critical portion of the device known as the "baseband processor" (BBP) that is used to connect to a telephone network and to utilize services on the network. By circumventing access controls on the OS, third parties could gain unauthorized access to the BBP, which could in turn result in gaining unauthorized access to and use of the telephone network or even causing operational damage to the network.

(3) The OS makes available functions and services to application programs through its APIs and system calls. Modifications to the OS can, whether intentionally or unintentionally, interfere with the proper operation of the APIs and system calls, causing application programs to fail to operate correctly on the phone. Moreover, updates to the OS distributed by Apple may not work correctly with modified earlier versions of the OS. When users attempt to update a device whose OS has been previously modified, serious functional problems can result, potentially causing the device to fail to operate.¹⁴⁴

4. PROPOSED REASONS FOR EXEMPTING JAILBREAKING FROM § 1201.

This article proposes three reasons the U.S. Copyright Office should grant an exemption for jailbreaking to be legal. First, circumventing technological protection measures for the lawful use of installing applications (jailbreaking) on one's iPhone is similar to the already listed exemption for the lawful use of connecting to a wireless

¹⁴⁴ Hayes, *supra* note 1 at 8-9.

network (unlocking). Second, jailbreaking causes little harm to Apple and actually provides it with benefits. And finally Jailbreaking allows for uses of the iPhone that are completely within the law, and so the Librarian of Congress should err on the side of accepting these assertions of noninfringement.

First, remedies still exist for consumers who use jailbreaking for unlawful purposes. If one uses a jailbroken iPhone to access “cracked” applications available from the App Store, he or she is violating the DMCA. But, since there are far more legal reasons to jailbreak an iPhone than illegal, and since the DMCA errs in favor of legal means to increase interoperability, the entire jailbreaking community should not be held in violation of the law when only a small number of consumers actually violate any of the policies behind the DMCA.

Moreover, the underlying policy behind Exemption Five granted by the Librarian of Congress, which allows for the unlocking of cell phones, is in line with the policy of an exemption that would allow for the jailbreaking of cell phones. Highlighted specifically in the LOC Notice was that wireless cell phone firmware locks restrict the ability of the cellular subscribers to change their service lawfully to a wireless carrier competitor. Just like the wording of Exemption Five, the Librarian of Congress could provide an exemption for the circumvention of firmware locks solely for the lawful use of application installation.

Since this was “a business decision unrelated to the interests protected by copyright” the Librarian ruled that this use was exempt from the law.¹⁴⁵ The prevention

¹⁴⁵Yoeli, *supra* note 2 at 95.

of jailbreaking, which simply allows applications not available through the App Store to be lawfully installed on a consumer's iPhone, is also "a business decision unrelated to the interests protected by copyright."¹⁴⁶ If Apple was truly concerned for protection of its copyright, it would sue those who are distributing its cracked applications, rather than fight for the ability of a consumer to lawfully customize its product. The obvious concern of Apple is maintaining its monopoly over the distribution of applications to its consumers. It's hard to blame the technological libertarians who want to choose applications from a competitive free market; the concern over malware for the technological libertarian is not enough to overcome the fear of App Store's monopoly.

Second, jailbreaking causes little harm to Apple and actually provides it with benefits. Apple's cost for malware repairs are not outweighed by the benefits Apple receives when consumers jailbreak. Apple does not cover the costs through its warranty, which prohibits coverage of any phone that has been jailbroken, and even one who would attempt to have a jailbroken phone repaired under warranty by Apple would need to restore the phone to its factory settings before Apple would look at the phone.¹⁴⁷ By restoring the phone before sending it to be repaired by Apple will in itself remove any malware that is rendering the phone inoperable.¹⁴⁸ Thus, Apple will not have to repair anything and so there should not be expenses imposed on Apple to repair jailbroken phones.

¹⁴⁶ *Id.*

¹⁴⁷ Apple iPhone Warranty *available at* http://images.apple.com/legal/warranty/docs/070808_iphone_Warranty.pdf.

¹⁴⁸ Apple.com, Backing up, updating, and restoring your iPhone and iPod touch software, Restoring Your iPhone or iPod Touch, <http://support.apple.com/kb/HT1414> (last visited Mar. 5, 2010).

Furthermore, Apple receives benefit when consumers jailbreak their phones so that they may run on networks other than AT&T. When a consumer buys an iPhone they are likely to sign a new contract with AT&T thus allowing them to receive the iPhone at a discounted price. But, if a consumer buys an iPhone without going through AT&T, and without receiving the discounted iPhone price, the consumer will need to pay full price for the iPhone. What Apple would normally sell for \$299 becomes \$699 every time a consumer wants to purchase a phone with the intent to jailbreak so that it may be used on other networks than AT&T.¹⁴⁹

Finally, Jailbreaking allows for uses of the iPhone that are completely within the law. The EFF made a compelling statement in its submission to the U.S. Copyright Office when it said “assertions of fair use or other statutory exceptions” that “lead the Librarian into areas that have not yet been addressed by the courts, the Librarian should err on the side of accepting these assertions of noninfringement, but narrow any resulting exemption to activities that are ultimately found by the courts to be noninfringing.”¹⁵⁰ This is compelling because there are many lawful uses that can be made from jailbreaking an iPhone. Accordingly, the Librarian of Congress is required to make a ruling every three years as a fail-safe mechanism to protect lawful uses of copyrighted works. Jailbreaking allows one to enjoy the iPhone beyond the factory restrictions by downloading programs made by third parties that consent to the downloading of their creations. Since there is nothing wrong with downloading programs as long as the

¹⁴⁹ Apple.com, iPhone – Apple Store (U.S.) <http://www.apple.com/iphone/buy/> (last visited Mar. 5, 2010).

¹⁵⁰ Lohmann, *supra* note 60 at 2.

copyright owner has consented, jailbreaking is just a process that makes use of this lawful practice.

CONCLUSION

The function of technological protection measures are put in place by Apple for various control purposes. “Unlocking” and “jailbreaking” an iPhone serves the interests of iPhone consumers because it increases the functionality of their purchased product. Protective measures that have been put in place by Apple to prevent the jailbreaking from happening seem to serve a business interest rather than a copyright protection interest. The law surrounding the processes of unlocking and jailbreaking, The Digital Millennium Copyright Act § 1201(a)(1), prohibits the circumvention of protection measures like the ones put in place on the iPhone by Apple. Even the § 1201(f) seems to fail due to the existence of a specific prohibition to reverse engineering in the Apple iPhone software licensing agreement. The three-year exemption ruling for 2009 has become a ruling for 2010 and the fate of jailbreaking legality is still unknown, however currently it stands not exempt and is technically illegal until the 2010 ruling decides the new legal status of this process.

The Electronic Frontier Foundation (“EFF”) and Apple fight a noble battle in that each attempts to fight for the protection and rights of consumers. Unfortunately for Apple, their concern for its consumer’s protection from malware becomes blurred when considering its interest in controlling its App Store monopoly. The reason why the Librarian of Congress should allow an exemption for jailbreaking an iPhone is grounded in the lawful purposes and uses of jailbroken iPhones. The Librarian of Congress herself

agreed to this policy when she exempted circumvention of technological protection measures for the purpose of lawfully connecting to a wireless carrier.