NOTE

THE IPHONE JAILBREAKING EXEMPTION AND THE ISSUE OF OPENNESS

*Michael H. Wolk**

The iPhone is a prominent example of an emerging breed of devices that use technological and legal protections to control the user experience. Apple locks down the iPhone by adding a gatekeeper in charge of determining what users can and cannot do with the device. Apple maintains that as the creator of the iPhone, it should be able to control the iPhone OS software, primarily to maintain a consistent user experience. Innovation advocates counter that, regardless of whether the user experience is positive for iPhone users, users should be able to choose to jailbreak their iPhones so that they can use their device as they see fit, instead of being limited to Apple-approved uses. The Digital Millennium Copyright Act currently reinforces Apple's legal grip on the iPhone OS. Policymakers interested in innovation should reconsider this results, and revise the DMCA's anti-circumvention rules accordingly.

* B.A., Colby College, 2007; J.D. Candidate, Cornell Law School, 2010. I would like to thank the editors and associates of the Cornell Journal of Law and Public Policy for their help throughout this process, Professor Oskar Liivak for his advice and feedback on this note, Danny Fischler for providing an extra set of eyes, Robert Zemeckis and Ivan Reitman for inspiring my curiosity and imagination, and Marcia, Dennis, and Dee for their love, patience, and support.

INTRODUCTION

On March 31, 2009, Skype, an online communications company, released an application for Apple's wildly popular iPhone.[1] Skype develops software for computers, stand-alone telephone devices, and mobile devices such as the iPhone that enables Skype users to conduct free or extremely low-cost phone calls to other Skype users or to landline and mobile numbers throughout the world.[2] Two days after the application was released, Skype announced that over one million copies of the program were downloaded, equivalent to roughly six downloads per second.[3] Although the high volume of initial downloads suggested significant interest in the application, there are some limitations to its operation that may have surprised Skype users. Skype for the iPhone connects calls only through a Wi-Fi connection cannot route calls over the phone carrier's wireless data network.[4] This means consumers can place Skype calls through the Wi-Fi network at Starbucks, but they will not be able to enjoy the same service in locations beyond the short reach

---

[1] *Today in Business*, N.Y. TIMES, Mar. 30, 2009, at B2.

[2] *See* Skype International Calling, http://www.skype.com/prices/callrates (last visited Mar. 7, 2010).

[3] Posting of Peter Parkes to Share Skype Blog, http://share.skype.com/sites/en/2009/04/skype_for_iphone_zooms_past_on.html (Apr. 2. 2009) (noting that "Skype for iPhone zooms past one million downloads").

[4] Ryan Kim, *App Connects iPhone Users with Skype*, S.F. CHRON., Mar. 31, 2009, at C1.

of a Wi-Fi connection.[5] The obvious question is, why? The answer is complicated, but the most basic reason is because Apple Inc. (Apple) is the gatekeeper of all iPhone software and, through legal and technical methods, the company only permits iPhone users to download Apple-approved software.[6] While this type of approach provides benefits for Apple, application developers, and iPhone users, I believe there are negative aspects of Apple's asserted control.

The introduction of the Skype application, or "app" in Apple's parlance, illustrates potential disadvantages of a "walled garden" or "appliancized" approach to consumer electronics.[7] A walled garden is a system where an entity controls as many aspects of a product as possible and where features are only available if approved by a central authority. In the case of the iPhone, Apple controls the manufacturing process, the operating system that runs on the phone, the software used by other parties to develop apps, and the store that serves as the sole conduit for delivering apps to consumers' phones.[8] From Apple's perspective, managing access to the iPhone is about controlling the quality and consistency of the consumer's experience using the device.[9] To this end, Apple took technological and legal steps to hamper the performance of certain tasks such as running unapproved apps or allowing consumers to take advantage of the iPhone operating system (OS) software's underly-

---

5 *See, e.g.*, FCC Radio Frequency Devices, 47 C.F.R. § 15.249 (2008), *available at* http://www.access.gpo.gov/cgi-bin/cfrassemble.cgi?title=200847; DANNY BRIERE & PAT HURLEY, WIRELESS NETWORK HACKS & MODS FOR DUMMIES 110 (2005) (noting the relatively weak strength of Wi-Fi signals).

6 *See Apple's Deal with AT&T Follows a 'Walled Garden' Strategy*, ECON. TIMES (India), July 9, 2008, http://www1.economictimes.indiatimes.com/articleshow/msid-3212643,flstry-1.cms (discussing Apple's model of control for the iPhone and how some experts view Apple's tight control over the device as a mistake); Chris Foresman, *Latest iPhone Developer Agreement Bans Jailbreaks*, ARS TECHNICA, Apr. 1, 2009, http://arstechnica.com/apple/news/2009/04/latest-iphone-developer-agreement-bans-jailbreaks.ars. *But see* Yukari Iwatani Kane, *Breaking Apple's Grip on the iPhone*, WALL ST. J., Mar. 6, 2009, a*vailable at* http://online.wsj.com/article/SB123629876097346481.html#.

7 *See* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 59–61 (2008) (describing an information appliance as a device which "remains tethered to its maker's desires, offering a more consistent and focused user experience at the expense of flexibility and innovation"); *Apple's Deal with AT&T Follows a 'Walled Garden' Strategy*, *supra* note 6. In this Note, I will primarily stick to the *walled garden* terminology as opposed to the possibly narrower terminology of *information appliances* or *appliancized hardware* as described in Professor Zittrain's *The Future of the Internet and How to Stop It*. According to Zittrain, the term *walled garden* may just refer to "a lack of interoperability" between systems while "information appliances" refers to contemporary tethered technology. E-mail from Jonathan Zittrain, Professor of Law, Harvard Law School and Kennedy School of Government, to Michael H. Wolk (Feb. 21, 2010, 00:51 EST) (on file with author).

8 Apple provides information about its App Store online. Apps for iPhone, http://www.apple.com/iphone/appstore/ (last visited Nov. 19, 2009).

9 *See infra* note 136 and accompanying text.

ing UNIX system to compile and run text editors and even web server software.[10]

Apple's strategy for controlling the iPhone includes the use of software and development contracts or licenses,[11] hardware and software technologies designed to ensure the iPhone is used only in the manner prescribed by Apple,[12] and protections under copyright law.[13] A key element of Apple's copyright protections is the threat of recourse for violating the anti-circumvention provisions of the Digital Millennium Copyright Act (DMCA).[14] The DMCA provides a cause of action, potentially steep fines, and criminal sanctions for defeating a technological protection measure (TPM) designed to protect access to a protected work, and it provides sanctions for trafficking in a "technology, product, service, device, component, or part thereof" that provides access to works protected by a TPM.[15] Apple argues that the DMCA protects against a controversial technique known as jailbreaking.[16] Jailbreaking enables iPhone users to change or modify the operating system running

---

10 I do not know why a user would want to run software such as the open-source Apache web server or Vim (a classic text editing program) on the tiny, low-powered iPhone other than to prove it is possible. Web server software is more typically run on computer systems with higher-performance hardware than that available on a laptop or portable computing device like the iPhone. Regardless, hackers were able to do so no later than July 25, 2007. Chad Shmukler, *Hacked iPhone Now Running Apache, Python, Vim*, IPHONEFAQ.ORG, July 25, 2007, http://www.iphonefaq.org/archives/97212.

11 *See, e.g.*, APPLE INC., IPHONE SOFTWARE LICENSE AGREEMENT (2009), http://images.apple.com/legal/sla/docs/iphone.pdf (describing restrictions on the consumers' use of the iPhone including a prohibition of modifying, reverse-engineering, and otherwise creating derivative works using the iPhone OS software). Also, the "iPhone Developer Program License Agreement" limits how a developer may use Apple's development products to produce apps. The license is not publicly available on Apple's site, however, one version is referenced in a news piece describing the addition of terms banning the act of jailbreaking as well as selling applications for jailbroken phones. Foresman, *supra* note 6. This Note does not explore the implications of the contracts and licenses ("Agreements") that bind iPhone owners and developers. Whether or not copyright law precludes the jailbreaking behavior discussed herein, there remain issues with the Agreements and other laws. For example, it is possible that a court might find jailbreaking to be a violation of the Agreements. On the other hand, the Agreements could potentially be preempted by copyright law. This Note's narrow scope, the implications of the Digital Millennium Copyright Act on jailbreaking, does not attempt to answer the wider question of whether jailbreaking violates any United States laws or the Agreements.

12 *See infra* Part I.B (discussing the iPhone TPMs).

13 *See infra* Part II (discussing the history and current applications of the DMCA).

14 17 U.S.C. § 1201 (2006).

15 *Id.* § 1201(a)(2). A civil cause of action for defeating a TPM is available in 17 U.S.C. § 1203, and 17 U.S.C. § 1204 provides for criminal sanctions. See 17 U.S.C. § 1203 (2006) (Defining civil remedies for violations of §§ 1201 and 1202); 17 U.S.C. § 1204 (2006) (Describing criminal penalties for certain willful violations of §§ 1201 and 1202). Section 1201(a)(2) is one of the DMCA's anti-trafficking provisions, and § 1201(a)(1)(A) provides the actual ban on the circumvention of a TPM. 17 U.S.C. § 1201(a)(2); 17 U.S.C. § 1201(a)(1)(A).

16 *See infra* notes 153 to 155 and accompanying text.

on the iPhone so that it is capable of performing tasks and running other software (such as a full-featured version of Skype) regardless of Apple's approval.[17]

While some commentators have argued that Apple's DMCA claims are quite weak,[18] this Note argues, despite my preference for permitting tinkering, that Apple will be able to rely on the DMCA to provide legal muscle in support of the iPhone's tethered control. This Note aims to examine the ongoing dispute over the legality of jailbreaking and to use this dispute to discuss some of the negative implications of today's DMCA policy. Part I presents background information on the use of TPMs, as well as a specific discussion of the protections employed on the iPhone. Part II examines the DMCA and the anti-circumvention rules. Part III analyzes the ongoing anti-circumvention waiver application for jailbreaking devices including the iPhone. Part IV steps back and analyzes how the DMCA has been and is likely to be applied, as well as the greater implications of this policy.

I. PROTECTION MEASURES

A. *Brief History of Copy Restrictions*

There is a long history of copyright holders working to prevent the electronic reproduction of their works. In the 1980s, a piece of hardware commonly referred to as a dongle was used as a key for unlocking software.[19] Dongle-protected software would not run on a computer unless the dongle was attached to one of the machine's ports.[20] Software licenses were sold with a single dongle, and this scheme made it difficult to run copied software on multiple machines since the software would only run if the dongle was connected to the computer.[21]

Similar attempts at copy control have been used for audio and video media. For example, technologies such as analog copy protection (ACP) prevent or distort the copying of protected content on the VHS format.[22]

---

17 *Id.*

18 Kane, *supra* note 6; *see infra* note 175.

19 Microprocessor for Executing Enciphered Programs, U.S. Patent No. 4,168,396 (filed Sept. 18, 1979); *see* BRUCE SCHNEIER, SECRETS & LIES: DIGITAL SECURITY IN A NETWORKED WORLD 251 (2000); J.D. Biersdorfer, *Q & A; The Mystery of the Dongle*, N.Y. TIMES, Oct. 15, 1998, at G4.

20 SCHNEIER, *supra* note 19, at 251.

21 *See generally id.* at 251–53 (describing how the dongle functions as a copy protection mechanism).

22 *See* Rovi ACP Guide, http://www.rovicorp.com/products/content_producers/protect/acp.htm (last visited Nov. 22, 2009). Once, unaware of ACP, I spent a long afternoon during eighth grade creating a compilation of short clips from Alfred Hitchcock films for a class presentation on the director. The ACP made the images on the VHS tape compilation oscillate in degrees of brightness.

More recently, record companies attempted to block compact disc copying by using copy protection technology.[23]

Today, companies commonly use as a means of protecting digital audio and video files sold over the internet. For example, Apple utilizes a type of TPM called FairPlay to regulate the use of audio files it sells through its iTunes store.[24] FairPlay-protected music can be played on Apple's iPod music players, on a limited number of authorized computers, and can be burned onto compact discs a limited number of times.[25] The iPhone, too, is capable of playing FairPlay-protected tracks.[26]

B. *iPhone TPMs and Protections*

Besides supporting protected media files, the iPhone has many layers of TPMs designed to control or prevent certain uses of the device, including two protections that are most relevant to this discussion.[27] First, the iPhone uses a technique called code signing as a part of a TPM designed to ensure that everything from the iPhone OS to the apps loaded on the phone have not been modified in any way.[28] Second, the iPhone OS is encrypted by Apple, and cannot be run on any device, including the iPhone, without being decrypted first.[29] The first sub-section will discuss these TPMs and how they are used on the iPhone. The following sub-section will discuss some common techniques used to modify the

---

23 CD copy prevention gained some notoriety after Sony BMG released over fifty different CD titles containing technology that unintentionally left Windows-based computers vulnerable to computer viruses. *See* Edward W. Felten & J. Alex Halderman, *Digital Rights Management, Spyware, and Security*, IEEE SECURITY & PRIVACY, Jan.–Feb. 2006, at 18–23 (describing Sony's copy protection technology).

24 Steve Jobs, Apple's CEO, posted an essay on February 6, 2007, describing Apple's current use of its FairPlay technology, and the resulting complications stemming from its use. Steve Jobs, *Thoughts on Music*, APPLE.COM, Feb. 6, 2007, http://www.apple.com/hotnews/thoughtsonmusic/.

25 About iTunes Store Authorization and Deauthorization, http://support.apple.com/kb/HT1420 (last visited Nov. 22, 2009) (explaining the authorization process for protected media).

26 Apple iPhone Technical Specifications, http://www.apple.com/iphone/specs.html (last visited Nov. 22, 2009) (describing ability to play protected AAC files, also known as FairPlay-protected M4P files).

27 This section will use the term *TPM* when referring to technical methods of restricting use of the iPhone device. While the definition of TPM is specific in the DMCA, part of the dispute addressed here depends on whether certain protections are actually TPMs protected by the DMCA. The term TPM is used here for the sake of simplicity, and its use is in no way an attempt to provide passive support for Apple's position. *See infra* Part I.B (discussing the iPhone's TPMs).

28 FRED VON LOHMANN & JENNIFER S. GRANICK, ELECTRONIC FRONTIER FOUNDATION, COMMENT: IN THE MATTER OF EXEMPTION TO PROHIBITION ON CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS FOR ACCESS CONTROL TECHNOLOGIES 7 (2008), *available at* http://www.copyright.gov/1201/2008/comments/lohmann-fred.pdf [hereinafter EFF COMMENT].

29 *Id.*

iPhone and defeat these TPMs and how these changes impact the operation of the iPhone device.

1. Integrity Through Code Signing

To ensure that it runs Apple-approved apps only, the iPhone incorporates a practice called code signing. Each app downloaded from the app store is code signed by Apple. Code signing uses a mathematical technique[30] to ensure that the app in use was distributed by Apple and that it has not been modified in any way.[31] While no computer authentication or security technique is foolproof, code signing is considered to be extremely reliable and is used in most modern operating systems.[32] Since code signing on its own is a method for testing data integrity, the iPhone's OS uses this technique to enforce a policy of only running properly signed apps. Every time a user attempts to run an app, the iPhone's OS performs an S-Check to enforce this policy. The S-Check functions as a gatekeeper that only runs an app if the S-Check can verify the App code's integrity through code signing in order to confirm the code was signed by Apple and was not subsequently modified.[33] Through the S-Check, Apple maintains its policy of control over the functionality of the iPhone by ensuring that consumers can only use Apple-approved apps.

2. Encryption

Portions of the iPhone OS are encrypted.[34] When an OS is stored in an encrypted form, its storage makes the software unusable and indecipherable until it has been decrypted back to its usable form. A simple analogy would be if one were to encrypt this Note. One could re-order every word (or letter) until the Note became an apparently meaningless

---

30 Code signing uses cryptographic hash functions. For a given hash function, and a given input, the resulting value is a constant. Any change in the input will lead to a different output. Because of these properties, a code signing technique can be used where a particular piece of software is used as the input for a hash function, and the output value is made available to the public on the producer's website or through some other means of public distribution. Savvy computer users can then run their copy of the software through the same hash function to ensure that their output value matches the official value. By using this method, a computer user can ensure they are using an unmodified version of the software. For a longer overview and useful sources, see JOHN VIEGA ET AL., NETWORK SECURITY WITH OPENSSL 192–95 (2002) (discussing hash functions).

31 For a quick overview and some helpful sources, see SCHNEIER, *supra* note 19, at 163.

32 *See* APPLE INC., MAC DEV CENTER, CODE SIGNING GUIDE (2009), *available at* http://developer.apple.com/mac/library/documentation/Security/Conceptual/CodeSigningGuide/CodeSigningGuide.pdf (offering a pared-down explanation of code signing, and how the technique is used in Apple's Mac OS X operating system).

33 The iPhone Dev Team produced a video explaining the jailbreaking process it uses in the software it releases. Internet Video: 25C3: Hacking the iPhone, http://video.google.com/videoplay?docid=7137637070605293O4 [hereinafter Dev Team Video].

34 *See id.* (stating that the kernel, a high-level component of the iPhone OS, is stored in an encrypted form on the iPhone's NAND flash memory).

series of alpha-numeric symbols. If one wished to then edit or understand the encrypted Note, one would have to decrypt, or reorder, the words first so that they could be understood. For jailbreaking the iPhone, the primary impact of iPhone OS encryption is that the operating system cannot be usefully modified until it is understood, and it cannot be understood until it is first decrypted.

3. Defeating TPMs and Running Non-Apple Approved Apps

There is more than one way to modify an iPhone in order to run outside apps. This section will focus on a jailbreaking technique used by a non-Apple-affiliated group called "iPhone Dev Team."[35] Much of the work performed by this group focuses on enabling the iPhone to run any program the user wants,[36] often by finding ways to defeat the S-Check.

Methods for defeating S-Check can be divided between those that rely on updateable iPhone OS software and those that rely on immutable hardware.[37] For software-based attacks,[38] one can take advantage of vulnerabilities or holes in the way the iPhone OS operates, bypass the S-Check process, and successfully run the desired software.[39] A problem with this type of exploit is that once a hole is discovered, Apple can fix it in a new version of the operating system. It may take a lot of time to research and find these errors, and so a battle ensues between the party trying to control (Apple) and those users who wish to break free of these restrictions.[40] Because Apple can patch software exploits, defeating S-Check in this manner becomes an exercise in futility.

---

35 *See* Dev-Team Blog, http://blog.iphone-dev.org/ (last visited Mar. 14, 2010). Some will refer to groups like iPhone Dev Team as hacker groups or hackers. The reason for doing so is based on negative connotations that are sometimes associated with the term *hack*. For example, the EFF, who supports a jailbreaking exemption, does not describe the activities as hacks or the participants as hackers. *See* EFF COMMENT, *supra* note 28. Apple, on the other hand, opposes the proposed exemption and has used these terms in order to suggest that the associated acts are dirty or illegal. *See* APPLE COMMENT, *infra* note 120. This is an unfortunate reality especially considering that today's hackers can also be viewed as the modern version of the previous generations of tinkerers who were just interested in how things work.

36 *See* Dev-Team Blog, *supra* note 35. The Dev Team provides information and software so that iPhone users can continue to run the latest official version of Apple's iPhone OS with modifications so they can run apps and other code from any source they choose. *Id.*

37 Defining what constitutes hardware versus software is not always straightforward, in part, because much of what can be accomplished using hardware can also be achieved through software. *See, e.g.*, ZITTRAIN, *supra* note 7, at 13–14 (comparing hard-wired hardware to software and noting that much of what can be embedded in hardware can also be achieved through software).

38 The term *attack* might evoke thoughts of violence, however, its use here is meant solely to describe methodologies for changing software's functionality.

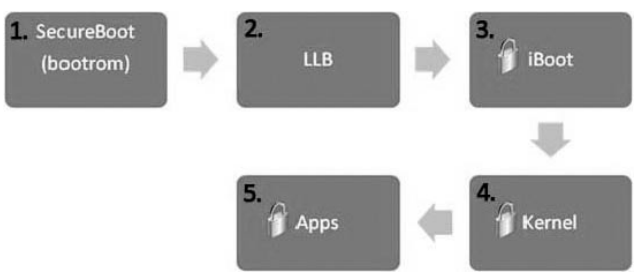
39 The specific exploit is not important and could be a stack overflow or similar code injection technique. *See* Dev Team Video, *supra* note 33.

40 A good example of this battle is an exploit purportedly used by a software company to allow users to install third-party apps on iPhones. The exploit worked through a vulnerability in the iPhone image processing software. The software, when reading an image, could be

As an alternative, groups such as iPhone Dev Team embraced a method that avoids this battle by exploiting the design of the iPhone's hardware instead of the more dynamic software.[41] Although Apple can update much of the iPhone OS to fix vulnerabilities, it cannot easily modify how the iPhone's hardware and low-level code operates.[42] As a result, exploits that rely on vulnerabilities at the hardware level avoid the back-and-forth fighting that occurs with exploits at the software level.[43]

One popular hardware-based method for overcoming the S-Check for apps is by undermining the S-Check early in the startup process. Apple protects the S-Check, which runs closer to the "surface" of the software by requiring successive code-checks by programs running "deeper" in the startup process.[44] Figure 1 diagrams the succession of programs that initiate when a user powers on the iPhone: SecureBoot must load the LLB, the LLB must load iBoot, iBoot must load the Kernel, and the Kernel is the program responsible for loading/running apps.[45]

FIGURE 1



The padlocks in Figure 1 affixed to Apps, Kernel, and iBoot show that those programs will function only if each passes a code signing check demonstrating the program's integrity.[46] This type of security

tricked into running code hidden in the image file. The code hidden in the image bypassed the S-Check, and made it possible to run unauthorized third-party apps on the iPhone. Once Apple fixed the image reading program in future versions of the iPhone OS, this vulnerability could not be exploited. *See* DAVID JURICK ET AL., iPHONE HACKS 8 (2008) (describing the back and forth as a cat-and-mouse scenario); Deconstructing the iPhone SDK: Malware, http://mikeash.com/?page=pyblog/deconstructing-the-iphone-sdk-malware.html (Mar. 20, 2008, 16:58).

41 *See* Dev Team Video, *supra* note 33.

42 *See id.*

43 *See* JURICK ET AL., *supra* note 40, at 15; Cat. Bag. Mouse., http://blog.iphone-dev.org/post/92185631/cat-bag-mouse (Apr. 2, 2009) (discussing how once a particular version of iPhone hardware is jailbroken, there is minimal difficulty in jailbreaking the device in the future because software updates do not impact the underlying vulnerability).

44 *See* JURICK ET AL., *supra* note 40, at 15.

45 *See id.*

46 *See id.*

scheme is known as a circle-of-trust model.[47] The reason someone seeking to run a third-party app cannot modify the Kernel to remove the S-Check is because the Kernel itself will not run unless the iBoot program has confirmed its integrity.[48] Similarly, the iBoot will not run unless the LLB first checks its integrity. This leads us to the hole in this chain. Although the LLB checks the integrity of the iBoot, no program checks the integrity of the LLB.[49] This makes it possible to modify the LLB so that it no longer checks the iBoot prior to its execution.[50] Once this occurs, the iBoot can also be modified. The Kernel can then be changed to disable S-Check and open the gate so that the iPhone will run apps or other code without any integrity check.[51]

While every detail of these exploits is not critical to the discussion, it is important to understand that there are many ways to enable the iPhone to run third-party apps. By defeating integrity checks at multiple levels, the method described above opens up the iPhone to running unofficial apps, as well as code that could compromise device security and other features designed to limit the impact of hardware malfunctions.[52] One final important detail is that each app sold through Apple's store is wrapped with a TPM designed to prevent iPhone users from using apps that they find elsewhere online or get from a friend (i.e. pirated apps).[53] These protections remain after jailbreaking; however, online software exists to remove this TPM from apps.[54] Once the protection is removed, these stripped apps can be run on any jailbroken iPhone, but not on unmodified devices.

4. Summary

Apple's use of TPMs on the iPhone follows in the footsteps of earlier copy protection technologies. Jailbreaking not only makes it possible to run unapproved apps, but it also opens the door for the installation and use of pirated copies of official apps for sale in the iTunes App Store.[55] The iPhone OS is not designed to distinguish between pirated apps and non-Apple-approved apps. Once the S-Check is removed, the

---

47 *See* CRICKET LIU & PAUL ALBITZ, DNS AND BIND 330 (5th ed. 2006) (describing use of chain-of-trust model in the context of securing DNS key-value pairs).

48 *See* Dev Team Video, *supra* note 33.

49 *See id.*

50 *See id.*

51 *See id.*

52 *See infra* note 138 and accompanying text (discussing arguments for protecting the iPhone).

53 *See* Erica Sadun, *App Store DRM Cracked, but What's the Point?*, ARS TECHNICA, Feb. 2, 2009, http://arstechnica.com/apple/news/2009/02/poetic-justice-watch-crackulous-released-pirated-re-sold.ars.

54 *Id.*

55 *See infra* note 138 (noting that jailbroken phones are often used for piracy purposes).

iPhone OS only distinguishes between apps from Apple, which arrive protected by a TPM tying the app to its purchaser, and those without such protections.[56] Thus, to take advantage of pirated apps, a consumer must have access to an unprotected version of the app (stripped of Apple's tying TPM)[57] and a jailbroken iPhone that does not check the integrity of apps, using S-Check, prior to their execution.[58]

II. DMCA

A. *History*

The contemporary copyright environment is one where many analog products such as books, VHS tapes, records, cassette tapes, and others have been supplanted by digital media such as e-books, compact discs (CDs), digital versatile discs (DVDs), and digital audio and video files. Unlike copies made from analog media, a digital copy is a perfect copy.[59] Thus, with digital copying, copies made from other copies have the same quality as the original digital file.[60]

Digital copy prevention technology may serve as an example of a tangible response to media owners' fears of digital copying and piracy. These TPMs can be applied to control the use of audio and video files sold or licensed to consumers through online stores.[61] For example, a consumer is limited to playing protected audio files from Apple's iTunes Store on a set number of computers and digital media players made by Apple.[62] Similarly, video files such as television episodes and movies are often wrapped with a TPM designed to limit the number of viewings and the types of devices that can access the content.[63] A key problem with TPMs is that users can defeat these technologies, enabling unencumbered distribution of previously protected content.[64] In response to the threat of digital copying, Congress passed the DMCA in hopes of

---

56 *See* Sadun, *supra* note 53.

57 *Id.*

58 *See* JURICK ET AL., *supra* note 40, at 14 (discussing the ability to use numerous third-party applications on jailbroken iPhones); Sadun, *supra* note 53.

59 *See* H.R. REP. No. 105-551, pt. 1, at 9 (1998) [hereinafter DMCA H.R. REP. I] (discussing the background and need for legislation).

60 *But see* Kevin Kelly, *Where Music Will Be Coming from*, N.Y. TIMES, Mar. 17, 2002, (Magazine), at 30.

61 Apple's iTunes Music Store is considered one of the first consumer-grade online stores capable of selling digital media while giving copyright holders the ability to control the use of protected audio files.

62 *See* Jobs, *supra* note 24 (noting that music files protected using Apple's FairPlay TPM may be played on 5 computers and an unlimited number of iPods).

63 *See* iTunes Store Movie Rental Usage Rights in the United States, http://support.apple.com/kb/HT1415 (last visited Feb. 28, 2010).

64 *See* Felten & Halderman, *supra* note 23, at 18–23.

providing a legal process to return control to the owners of copyrighted works.[65]

B. *The Act*

The DMCA's anti-circumvention provisions make it illegal to bypass TPMs designed to protect copyrighted content.[66] Specifically, § 1201(a)(1)(A) provides: "No person shall circumvent a technological measure that effectively controls access to a work protected under this title."[67] The remainder of § 1201 defines relevant terms and provides specific exceptions to the DMCA's anti-circumvention rules whereby a TPM may be defeated without incurring liability. The act defines circumventing protections afforded by a technological measure as, "avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure."[68] Further, "a technological measure 'effectively protects a right of a copyright owner under this title' if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title."[69] Thus, a key element to the validity of a TPM is whether it is truly protecting an underlying copyright.[70]

In addition to prohibiting the act of circumvention, the DMCA bans trafficking in products that are primarily used for circumventing a TPM.[71] Although individuals, sitting in the privacy of their homes, can circumvent a TPM, the anti-trafficking prohibition targets more public behaviors: "No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof . . . ."[72]

The remainder of this anti-trafficking provision defines the prohibited products or services.[73] The scope of the banned products is those with "only limited commercially significant purpose or use other than to

---

65 *See* DMCA H.R. REP. I, *supra* note 59, at 9–11.

66 *See id.* at 14.

67 17 U.S.C. § 1201(a)(1)(A) (2006).

68 *Id.* § 1201(b)(2)(A).

69 *Id.* § 1201(b)(2)(B).

70 This issue can be rather confusing because of the many ways computer code may be used in digital devices. *See, e.g.*, Davidson & Assocs. v. Jung, 422 F.3d 630, 640–41 (8th Cir. 2005) (citing Lexmark v. Static Control Components, 387 F.3d 522, 546 (6th Cir. 2004) (finding an authentication sequence contained on printer cartridge chips is not a TPM protecting access to Lexmark's "Toner Load Program" and its "Printer Engine Program")); Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1203–04 (Fed. Cir. 2004) (holding that a company specializing in replacement garage door openers did not violate the DMCA in distributing a replacement opener compatible with Chamberlain doors).

71 17 U.S.C. § 1201(a)(2).

72 *Id.*

73 *Id.* § 1201(a)(2)(A)–(C) (describing two classes of goods or services that would violate the DMCA).

circumvent a [TPM]."[74] The legislative record shows that this section was aimed at "black box" circumvention technology[75] the purpose of which is primarily the circumvention of TPMs.[76] Furthermore, the record states that anti-trafficking language is not aimed at "products that are capable of commercially significant non[-]infringing uses, such as consumer electronics, telecommunications, and computer products—including videocassette recorders, telecommunications switches, personal computers, and servers—used by businesses and consumers for perfectly legitimate purposes."[77]

C. *DMCA Exemption Process*

The DMCA has been criticized for its broad protections and for prohibiting uses of copyrighted works that would otherwise be legal if the works were not protected by the act.[78] For example, a film professor may wish to take clips from several films on DVD and burn them onto a single disc for quick presentation during class time.[79] While such an act is likely fair use, the necessary circumvention of the DVD's TPM would be a violation of the DMCA. In an attempt to soften these potentially harsh results, § 1201(a)(1)(C) provides for a notice and comment rulemaking process for exemptions to the DMCA's anti-circumvention rules. The statute provides several factors for the Library of Congress to consider when evaluating whether to grant a particular request:

i. the availability for use of copyrighted works;

---

74 *Id.* § 1201(a)(2)(B).

75 Examples of cases involving "black box" technologies include DVD circumvention products as well as chips and other devices used to circumvent TPMs designed to ensure that video game systems will not play pirated games. Sony Computer Entm't Am., Inc. v. Filipiak, 406 F. Supp. 2d 1068, 1076–77 (N.D. Cal. 2005) (finding defendant liable for trafficking devices designed to modify Sony's Playstation video game hardware in order to circumvent a TPM preventing the use of copied games); 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085, 1099 (N.D. Cal. 2004) (holding that 321 Studios' DVD Copy Plus program violated the anti-circumvention provisions of the DMCA).

76 H.R. REP. No. 105-551, pt. 2, at 38 (1998).

77 *Id. See generally* Posting of Sarah McBride & Yukari Iwatani Kane to Digits, http://blogs.wsj.com/digits/2009/04/24/realnetworks-and-hollywood-spar-over-dvd-ripping/tab/article/ (Apr. 24, 2009, 04:11 EST) (demonstrating that the line between so-called "black box" infringement devices and the second class of permitted products is not nearly as crystal clear as it was believed when the DMCA was enacted).

78 *See* Steven P. Calandrillo & Ewa M. Davison, *The Dangers of the Digital Millennium Copyright Act: Much Ado About Nothing?*, 50 WM. & MARY L. REV. 349, 350 (2008).

79 This specific issue was addressed in 2006 (and mentioned in the Calandrillo & Davison article, *supra* note 78), and the Library of Congress granted an exemption because otherwise it would be a violation of the DMCA because of the content scrambling system (CSS) protections used to protect DVD content. MARYBETH PETERS, U.S. COPYRIGHT OFFICE, RECOMMENDATION OF THE REGISTER OF COPYRIGHTS IN RM 2005-11: RULEMAKING ON EXEMPTIONS FROM PROHIBITION ON CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS FOR ACCESS CONTROL TECHNOLOGIES 1 (2006), *available at* http://www.copyright.gov/1201/docs/1201_recommendation.pdf [hereinafter 2006 RECOMMENDATION].

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.[80]

The Library of Congress has conducted three rulemakings. A fourth rulemaking, while due at the end of 2009, has not yet been promulgated at the time this note went to press in 2010.[81] In the most recent 2006 rulemaking, the Library announced the exemption of six classes of copyrighted works from the protections provided by the DMCA.[82] These classes include exemptions for media studies and film professors who want to circumvent protections on certain audiovisual works in order to make compilations for the classroom,[83] and also for any person who uses computer programs for the sole purpose of unlocking mobile telephones.[84]

III. JAILBREAKING EXEMPTION

This Part discusses an exemption recently proposed by the Electronic Frontier Foundation (EFF). In the current 2008–2010 rulemaking, the EFF proposed renewal of the exemption for unlocking mobile telephones discussed in the previous Part of this Note.[85] Additionally, it proposed an exemption that encompasses the activities necessary to jail-

---

80 17 U.S.C. § 1201(a)(1)(C)(i)–(v) (2006). In the 2006 Recommendation, the Librarian explained that the additional factors referred to in the fifth paragraph "require the Register to carefully balance the availability of works for use, the effect of the prohibition on particular use and the effect of circumvention on copyrighted works." 2006 RECOMMENDATION, *supra* note 79, at 5.

81 The U.S. Copyright Office, Rulemaking on Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works, http://www.copyright.gov/1201/ (last visited Nov. 23, 2009).

82 Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68,472, 68,472 (Nov. 27, 2006) (to be codified at 37 C.F.R. pt. 201).

83 *Id.* at 68,473–74.

84 *Id.* at 68,476; *see, e.g.*, John Haubenreich, *The iPhone and the DMCA: Locking the Hands of Consumers*, 61 VAND. L. REV 1507, 1513 (2008) (discussing the DMCA exemption for unlocking mobile devices and the current 2008–2009 rulemaking). It is not entirely clear whether the 2006 phone unlocking exemption is an anomaly resulting from the mobile phone industry's failure to file their comments on time or whether the Library of Congress will renew the exemption in 2009 having had the chance to review arguments on both sides this time.

85 *See infra* Part III.A.

break an iPhone for the purposes of running unapproved software programs, such as third-party apps.[86]

The EFF proposed a new class of exempted copyrighted works: "computer 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."[87] This Part will review the EFF's arguments in favor of this exemption, Apple's claims against such a grant, and other arguments that provide further perspective on this issue. Apple's and the EFF's comments discuss the applicability of 17 U.S.C. § 117, fair use, and the weight of the anti-circumvention factors listed in § 1201(a)(1)(C). As a result, the following discussion will focus primarily on these three areas while attempting to provide a meaningful account of each side's overall argument.

A. *Electronic Frontier Foundation (EFF)*

EFF describes itself as a member-supported non-profit with an interest in seeking a balance to copyright laws in order to protect the interests of copyright owners and the public.[88] For this exemption, The EFF broadly argued that "there is no copyright-related rationale for preventing iPhone owners from decrypting and modifying the device's firmware in order to enable their phones to interoperate with applications lawfully obtained from a source of their own choosing."[89] The EFF presented three arguments for why jailbreaking does not actually infringe a copyright.

1. Jailbreaking Methods Vary

First, it argued that some types of jailbreaking do not violate the software license because the methods do not involve decrypting, modifying, or creating a derivative work of the iPhone OS.[90] The EFF admits that some modifications do require decrypting the iPhone OS, but argues it is not clear whether these acts constitute a modification in violation of the license agreement or whether the addition of code without changing

---

86 *See id.*

87 EFF COMMENT, *supra* note 28, at 1. The wording here is interesting given that this language would not extend to devices like the iPod Touch which appears functionally equivalent to the iPhone, but lacks built-in telephone capabilities. *Compare* iPod Touch Technical Specifications, http://www.apple.com/ipodtouch/specs.html (last visited Apr. 12, 2010) *and* iPhone Technical Specifications, http://www.apple.com/iphone/specs.html (last visited Apr. 12, 2010).

88 *Id.*

89 *Id.* at 5.

90 *See id.* at 8.

any of the programs that make up the iPhone OS is just "using the iPhone" as authorized in the software license agreement.[91]

2. Section 117

Secondly, the EFF argued that under 17 U.S.C. § 117, it is permissible for iPhone owners to adapt their legally obtained copies of the iPhone OS so long as the changes do not, "harm the interests of the copyright proprietor."[92] The EFF maintains that *Krause v. Titleserv, Inc.*[93] provides an analogous example of a license-holder being permitted to modify licensed software in order to adapt it to meet current business needs.[94]

3. Fair Use

Thirdly, the EFF argued that the use at issue falls within the fair use exception defined in 17 U.S.C. § 107. Under § 107, a court should consider the following fair use factors:

i. the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
ii. the nature of the copyrighted work;
iii. the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
iv. the effect of the use upon the potential market for or value of the copyrighted work.[95]

With regard to these factors, the EFF insisted some weigh in its favor while others do not fit into this particular analysis.[96] It argued that the first factor weighs in favor of fair use since jailbreaking is a noncommercial, private act by individual users.[97]

---

91 *See id.* One could perhaps view this distinction analogously using a jelly bean hypothetical. First, imagine a handful of red jelly beans. If someone were to add a few blue jelly beans without taking away any red, is the handful still a handful of red jelly beans or have the blue turned it into something new? The EFF is arguing that adding a few blue jelly beans is not a modification since all of the red beans are still in the handful. If an operating system is viewed as a collection of programs, and someone adds a few additional items to this grouping, it is not entirely clear whether this constitutes a modification since no individual program is changed.

92 EFF COMMENT, *supra* note 28, at 9 (citing Krause v. Titleserv, Inc., 402 F.3d 119, 127–29 (2d Cir. 2005) (holding that Titleserv, which paid Krause to develop computer programs for its sole benefit, was exempted, through 17 U.S.C. § 107(a), from copyright liability for modifying some of Krause's programs to address bugs, adapt the programs for use with Microsoft Windows, and add new capabilities that made the software more responsive to Titleserv's business needs)).

93 402 F.3d 119 (2d Cir. 2005).

94 *See* EFF COMMENT, *supra* note 28, at 9 (citing *Krause*, 402 F.3d at 127–29).

95 17 U.S.C. § 107 (2006).

96 *See* EFF COMMENT, *supra* note 28, at 9.

97 *See id.*

Without specific citations, the EFF stated that the second and third factors are of reduced importance in cases involving private, noncommercial uses.[98] For the second factor, it noted that courts have found fair use in cases of software modification even though such modification requires copying both the functional and creative elements of the iPhone OS software.[99]

For the fourth factor, the EFF explained that the relevant work is the iPhone OS and notes that it is not sold separately from the iPhone hardware and is available for free on Apple's website.[100] Based on these facts, the EFF argued that the iPhone OS has no independent economic value except for its use on the iPhone, and if users learn they can jailbreak iPhones to run third-party software, demand for the iPhone, and thus the iPhone OS, will only increase.[101]

The EFF concluded by noting that while any of the three arguments presented should be sufficient to demonstrate that jailbreaking is noninfringing, it is possible for changes in the specific facts to alter the outcome of these arguments.[102] Perhaps because of the factual dependence of this type of inquiry, the EFF stated that "[g]ranting an exemption to § 1201(a)(1)'s circumvention prohibition is the proper way to permit non-infringing uses of jailbroken iPhones while affording courts the opportunity to reach undecided issues."[103]

4. Section 1201(a)(1)(C) Factors

After making its three arguments, the EFF discussed the § 1201(a)(1)(C) factors and how they relate to the proposed jailbreaking exemption. For the first factor,[104] the availability for use of copyrighted works, the EFF made an argument analogous to the fourth factor argument under the fair use doctrine.[105] It argued that since the iPhone OS has no economic value independent from the iPhone hardware, and since allowing people to jailbreak will likely increase demand, then the availability of such firmware will be enhanced because of increased demand for the iPhone and its underlying software.[106] Citing the 2006 rulemaking, the EFF stated, "the software locks that prevent phone owners from

98 *See id.* at 10.

99 *See id.* (citing Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510, 1524–26 (9th Cir. 1993)).

100 *See id.* at 9.

101 *See id.*

102 *See* EFF COMMENT, *supra* note 28, at 9.

103 *Id.* In other words, if the exemption were granted, parties with fair uses could then proceed with those uses without the risk of violating the DMCA anti-circumvention cause of action.

104 17 U.S.C. § 1201(a)(1)(C)(i) (2006); *see supra* note 80 and accompanying text.

105 *See* EFF COMMENT, *supra* note 28, at 10–11.

106 *See id.* at 11 (citing 2006 RECOMMENDATION, *supra* note 79, at 52).

running software of their choosing are not intended to protect the market for copyrighted firmware—instead, these software locks are intended to 'control the use of hardware which, as is increasingly the case, may be operated in part through the use of computer software or firmware.'"[107] Along these lines, it continues to argue that while it does not believe the iPhone's availability will be harmed, consumers will be harmed because they lack an alternative for running third-party apps on their devices.[108]

For the second factor,[109] the availability for use of works for non-profit archival, preservation, and educational purposes, the EFF briefly stated that it is unlikely that jailbreaking will impact the availability of the iPhone OS for the respective uses listed in this factor.[110]

For the third factor,[111] the impact on criticism, comment, news reporting, teaching, scholarship, or research, the EFF argued that while the inability to jailbreak smartphones may impact the listed uses, the granting of an exemption for jailbreaking would not have an adverse impact.[112]

For the fourth factor,[113] the effect on the market for, or value of, copyrighted works, the EFF again argued that the market for the iPhone OS will not be adversely impacted.[114] Besides repeating its argument that demand for the iPhone and iPhone OS will increase if jailbreaking is permitted, the EFF also addressed concerns that jailbreaking will impact the TPMs used to protect audio-visual media and apps.[115] The EFF pointed out that the TPMs used to protect media, as well as the technology used to prevent copying of apps from Apple's official store, are in no way impacted by jailbreaking.[116] Those protections are separate; and the jailbreaking process does not involve tampering with those TPMs.[117]

The EFF concluded its argument by quoting a passage from the 2006 Recommendation of the Register of Copyrights:

> [W]hen application of the prohibition on circumvention of access controls would offer no apparent benefit to the author or copyright owner in relation to the work to which access is controlled, but simply offers a benefit to a third-party who may use § 1201 to control the use of

---

107 *Id.* (citing 2006 RECOMMENDATION, *supra* note 79, at 52).
108 *See id.*
109 17 U.S.C. § 1201(a)(1)(C)(ii); *see supra* note 80 and accompanying text.
110 *See* EFF COMMENT, *supra* note 28, at 11.
111 17 U.S.C. § 1201(a)(1)(C)(iii); *see supra* note 80 and accompanying text.
112 *See* EFF COMMENT, *supra* note 28, at 11.
113 *See supra* note 80 and accompanying text.
114 *See* EFF COMMENT, *supra* note 28, at 11–12.
115 *See id.*
116 *See id.*
117 *See id.*

> hardware which, as is increasingly the case, may be operated in part through the use of computer software or firmware, an exemption may well be warranted.[118]

The EFF argued that this comment, taken from the Register of Copyright's recommendation supporting the currently enacted mobile phone unlocking exemption, should apply in the jailbreaking context.[119]

B. *Apple*

Unsurprisingly, Apple made a forceful argument against permitting a jailbreaking exemption in its response to the EFF's proposal. It claimed that any circumvention exemption:

> will destroy the technological protection of Apple's key copyrighted computer programs in the iPhone device itself and of copyrighted content owned by Apple that plays on the iPhone, resulting in copyright infringement, potential damage to the device and other potential harmful physical effects, adverse effects on the functioning of the device, and breach of contract."[120]

Apple also broadly argued that the EFF has not met its "burden of proof for demonstrating harm to non-infringing uses of the copyrighted works" protected by the iPhone TPMs, and that no interoperability exemption is necessary because interoperability is already explicitly addressed in § 1201(f) of the DMCA.[121]

Apple's position is that the EFF's argument is really an attack on Apple's business choices on the basis of inappropriate economic and social considerations.[122] It views the EFF's proposed exemption as an attempt to acquire government approval for transforming the proprietary computing platform into one capable of using third-party applications without demonstrating how such a change would "increase innovation or

---

118 *Id.* at 12 (quoting 2006 RECOMMENDATION, *supra* note 79, at 52).

119 *See* EFF COMMENT, *supra* note 28, at 12.

120 DAVID L. HAYES, APPLE INC., RESPONSIVE COMMENT IN OPPOSITION TO PROPOSED EXEMPTION 5A AND 11A 2 (2009), *available at* http://www.copyright.gov/1201/2008/responses/apple-inc-31.pdf [hereinafter APPLE COMMENT].

121 *See id.* at 2. Note that this paper has not distinguished between the iPhone OS software code that is stored on the read-only system memory and the "hardware-level" code such as the bootloader. The EFF's comments refer to the sum of these creations as iPhone firmware. Apple appears to distinguish the operating system from code like the bootloader but describes both as computer programs. *Id.* at 6–7 (describing the iPhone OS and the bootloader). Here, such distinctions should not have an impact, though it is worth pointing out the distinction since Apple makes one in its comments, and since Figure 1 refers to several programs (SecureBoot, LLB, and iBoot) that may or may not come within the scope of what Apple defines as the bootloader. *Id.* at 11–13.

122 *See id.*

investment in creative works."[123] Apple's position is that a decision by the Copyright Office would be inappropriate because the office is not qualified or supposed to consider the social value of business arrangements.[124] Even if the Copyright Office were to consider economic or social arguments, Apple argued that the EFF failed to establish that a jailbreaking exemption would have such a result and then stated that the exemption would actually be quite detrimental to the iPhone experience.[125] The following sections examine Apple's responses to the EFF's claims regarding 17 U.S.C. § 117, eligibility for fair use, and the § 1201(a)(1)(C) anti-circumvention factors.

1. Section 117

Apple argued that the EFF incorrectly applied § 117(a) to the iPhone for four reasons.[126] First, although no court has directly considered the issue, Apple pointed to a report,[127] used by nearly all courts examining § 117(a) issues, that states that § 117(a) rights may be negated by contract law.[128] A jailbreaking exemption would harm Apple because jailbreaking violates the rights reserved in Apple's software licenses.[129]

Second, Apple noted that jailbreaking tools, including the iPhone Dev Team's PwnageTool, do not modify the consumer's own copy of the iPhone OS.[130] Instead, some of these tools install a previously prepared iPhone OS modification that is incorporated into a copy of the jailbreaking software.[131] Thus, the modified iPhone OS installed by these tools is not licensed to the numerous people who then download it and use it to modify their iPhones. Apple argues that these tools violate § 117(a) because that section requires the owners of a copy of a computer program to either make the adaptation themselves or authorize the making of the

---

123 *See id.*

124 *See id.* at 3.

125 *See id.*

126 *See id.* at 13.

127 NATIONAL COMMISSION ON NEW TECHNOLOGICAL USES OF COPYRIGHTED WORKS, FINAL REPORT 13–14 (1978) [hereinafter CONTU Report].

128 *See* APPLE COMMENT, *supra* note 120, at 14.

129 *See id.*

130 *See id.*

131 *See id.* There is a distinction between modifying a copy of the iPhone OS licensed to you and modifying a copy of the software licensed to someone else and then shared with others. While both copies are identical, sharing a modified version of your own copy of the OS with someone else, even if they legally possess their owned licensed copy, might be viewed as a violation of copyright law. *See, e.g.*, UMG Recordings, Inc. v. MP3.Com, Inc., 92 F. Supp. 2d 349, 350 (S.D.N.Y. 2005) (stating that it is a "presumptive case of infringement" for a company to stream songs from its own copy of an album with individuals who also have their own copy of the same album).

adaptation on their behalf.[132] Furthermore, Apple pointed out that according to § 117(a), adaptations "may be transferred only with the authorization of the copyright owner."[133] Apple has not authorized these uses.

Third, recent § 117 opinions have permitted some software adaptation in order to add certain features.[134] A limitation on this right is that it may "only be exercised so long as [the modifications do] not harm the interest of the copyright proprietor."[135] Apple raised numerous concerns with the potential for adverse hardware effects from modified software: ensuring users have a "consistently good experience with the product"; handling support issues related to jailbroken iPhones, which increase call volume and the overall cost of its support infrastructure; and coping with the diminished value of the iPhone to Apple and third-party developers now that jailbroken phones can run unauthorized pirated copies of copyrighted software.[136]

Fourth, Apple pointed to *Krause* where the court stated, "[w]hether a questioned use is a use *in another manner* seems to us to depend on the type of use envisioned in the creation of the program."[137] Apple noted that it designed its system to function in a manner that preserves operational integrity and avoids the "many potential problems that unauthorized modifications cause."[138]

2. Fair Use

With regard to the first fair use factor, the purpose and character of the use,[139] Apple noted that although individual use of a modified iPhone is a personal use, such use is not transformative, and should be considered a commercial use because jailbroken phones are often used to play pirated content that would otherwise only be available by purchasing a licensed copy.[140] Based on these alleged facts, Apple argued that the first factor weighs against fair use.

---

132 *See* APPLE COMMENT, *supra* note 120, at 14 (citing Krause v. Titleserv, Inc., 402 F.3d 119, 122 (2d Cir. 2005)).

133 *See id.* at 15 (citing Midway Mfg. Co. v. Strohon, 564 F. Supp. 741, 745 n.2 (N.D. Ill. 1983) ("Section 117 'is not authority for [defendant's] sales of reproductions of [plaintiff's] program as adapted.'").

134 *See id.*

135 *Id.* (citing *Krause*, 402 F.3d at 129).

136 *See id.* at 16.

137 *Id.* at 17 (citing *Krause*, 402 F.3d at 129).

138 APPLE COMMENT, *supra* note 120, at 17.

139 17 U.S.C. § 107 (2006); *see supra* note 95 and accompanying text.

140 *See* APPLE COMMENT, *supra* note 120, at 17 (citing Wall Data Inc. v. L.A. County Sherriff's Dep't, 447 F.3d 769, 778–79 (9th Cir. 2006)). In *Wall Data v. L.A. County Sheriff's Dep't*, the Ninth Circuit found a commercial use where the party copied software licensed for one computer onto many computers. *Id.* Apple argued that because jailbreaking can enable piracy that is not possible on an unmodified iPhone, the fact that some people use jailbroken

For the second fair use factor, the nature of the copyrighted work, and the third factor, the amount and substantiality of the portion used in relation to the copyrighted work as a whole,[141] Apple stated that the iPhone OS is highly creative in nature and jailbreaking modifications involve copying nearly the entire work.[142] Thus, these two factors weigh against finding fair use.[143] For the fourth fair use factor, the effect of the use upon the potential market for or value of the copyrighted work,[144] Apple restated its arguments regarding the harm that jailbreaking does to its interests and how this diminishes the value of the iPhone OS for Apple.[145]

In addition, Apple responded to some of the EFF's fair use assertions.[146] In particular, Apple argued that the claim that the iPhone OS has no independent economic value[147] is misleading since the iPhone OS is not a product but a component of the "iPhone mobile computing product."[148] Apple noted that the iPhone OS's value is as software for the iPhone platform, and that the value of the iPhone OS software is a function of the number and quality of apps developed for the iPhone device.[149] Apple believes that incentivizing the creation of a high volume of quality apps is a function of the protections provided by the iPhone OS, which ensure safe and secure app distribution.[150] Apple finished its fair use discussion by stating that the EFF's proposed exemption lacks any evidence that an exemption permitting removal of Apple's TPMs will produce a net societal benefit by increasing investment in copyrighted works as compared to Apple's current iPhone strategy.[151]

3. Section 1201(a)(1)(C) Factors

Prior to discussing the weight of the fair use factors, Apple responded to the EFF's characterization of the 2006 mobile phone unlocking exemption[152] by arguing that the EFF has construed a meaning that ignores the original context.[153] In particular, Apple views the exemption

iPhones to run pirated software is sufficient to show an analogous commercial nature similar to the one present in *Wall Data*. *Id.* There is clearly a difference between the acts at issue in *Wall Data* and the mixture of potential problems with jailbreaking.

141 17 U.S.C. § 107; *see supra* note 95 and accompanying text.
142 *See* APPLE COMMENT, *supra* note 120, at 17.
143 *See id.*
144 17 U.S.C. § 107; *see supra* note 95 and accompanying text.
145 *See* APPLE COMMENT, *supra* note 120, at 18.
146 *See id.*
147 *See* EFF COMMENT, *supra* note 28, at 9.
148 APPLE COMMENT, *supra* note 120, at 18.
149 *See id.*
150 *See id.*
151 *See id.*
152 *See supra* note 118 and accompanying text.
153 *See* APPLE COMMENT, *supra* note 120, at 21.

narrowly and believes it only applies where the TPM does not protect a copyrighted work.[154] Apple views its TPMs as protecting its copyright interest in the iPhone OS, along with its overall interest in maintaining product integrity.[155]

For the first factor,[156] the availability for use of copyrighted works, Apple argued the availability for non-infringing purposes will not be impacted because the acts at issue in the proposed exemption are infringing.[157] Apple also argued that the TPMs at issue here promote the creation of copyrighted works.[158] First, the TPMs ensure integrity, and that incentivizes Apple and its potential competitors to produce products like the iPhone which may otherwise be more expensive to support.[159] Second, the TPMs support the iPhone ecosystem which incentivizes development of creative works (apps) by providing infrastructure for development, distribution, and monetization.[160] Apple noted that it reviews submitted apps to ensure that they meet certain standards and that they do not present any security or compatibility issues.[161]

For the second factor,[162] the availability for use of works for nonprofit, archival, preservation, and educational purposes, Apple argued that the harms discussed in the previous factor may have a detrimental effect on the availability concerns for this factor.[163] Those harms will decrease incentives for the creation of products like the iPhone and software that runs on those devices.[164] With a lower output of creations, the sum of works available for nonprofit archival, preservation, and educational purposes may be harmed.[165]

Apple then went on to argue each remaining factor either weighed in its favor or should have no weight. For the third factor,[166] the impact on criticism, comment, news reporting, teaching, scholarship, or re-

---

154 *See id.*

155 *See id.* at 22; *supra* note 130 and accompanying text.

156 17 U.S.C. § 1201(a)(1)(C)(i) (2006); *see supra* note 80 and accompanying text.

157 *See* APPLE COMMENT, *supra* note 120, at 22.

158 *See id.*

159 *See id.* In other words, Apple believes that if the costs related to the use of the iPhone are increased for creators like Apple, fewer companies may enter the market or attempt to create similar products. *Id.* The value of the iPhone and its OS is reduced if Apple must bear the cost of support infrastructure and customer calls that relate to problems stemming from undesired jailbreaking modifications. *Id.* Apple states that this is already a problem, and that the problem may only get worse if the Library of Congress were to permit a jailbreaking exemption. *Id.*

160 *See id.* at 23.

161 *See id.* at 24.

162 17 U.S.C. § 1201(a)(1)(C)(ii) (2006); *see supra* note 80 and accompanying text.

163 *See* APPLE COMMENT, *supra* note 120, at 25.

164 *See id.* at 22–24.

165 *See id.* at 25.

166 17 U.S.C. § 1201(a)(1)(C)(iii); *see supra* note 80 and accompanying text.

search, Apple agreed with the EFF that a jailbreaking exemption would have little impact on these factors.[167] For the fourth factor,[168] the effect on the market for, or value of, copyrighted works, Apple referenced its prior discussion[169] arguing that jailbreaking will reduce the incentives for the creation of copyrighted works like the iPhone OS, as well as other works like apps which, without proper protections, are more likely to be pirated by iPhone users.[170] For the remaining catch-all factors,[171] Apple argued it might be unwise to create an interoperability exemption since Congress has already spoken on the issue in § 1201(f).[172] Apple ends its discussion by re-emphasizing that it believes the EFF has failed to demonstrate the required harm.[173]

C. *Other Views on the Proposed Exemption*

Since the exemption process is ongoing and many of the filings and comments discussed here have only been available for a matter of months, there is little available scholarship on the proposed exemption.[174] One author, Ryan Witte, argues that an exemption should be granted based solely on a fair use analysis.[175]

Specifically, Witte argues that three of the four fair use factors weigh in favor of a jailbreaking exemption.[176] For the first fair use factor, the purpose and character of the use,[177] Witte aligns with the EFF in arguing that the nature of the use is personal, and since jailbreaking software, like PwnageTool, is distributed without any financial gain, the factor should favor a fair use exemption.[178]

As to the second fair use factor, the nature of the copyrighted work,[179] Witte compares iPhone TPMs to the protections at issue in *Lexmark Int'l Inc. v. Static Control*.[180] Witte argues that to the extent

---

167 *See* APPLE COMMENT, *supra* note 120, at 25.

168 17 U.S.C. § 1201(a)(1)(C)(iv); *see supra* note 80 and accompanying text.

169 *See* APPLE COMMENT, *supra* note 120, at 12.

170 *See id.* at 25.

171 17 U.S.C. § 1201(a)(1)(C)(v); *see supra* note 80 and accompanying text.

172 *See* APPLE COMMENT, *supra* note 120, at 25.

173 *See id.* at 25–26. The requisite harm issue is outside of the scope of this Note and so the details of the EFF's and Apple's claims regarding the related burden are omitted.

174 As of February 19, 2010, the Library of Congress has yet to publish its rulemaking; it was originally due at the end of October 2009.

175 Ryan Benjamin Witte, *Breaking Out of Section 1201(a) Liability: Why Jailbreaking the iPhone Constitutes Fair Use Under Copyright*, (unpublished working paper), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1371863.

176 *See id.* at 11.

177 17 U.S.C. § 107(1) (2006); *see supra* note 95 and accompanying text.

178 *See* Witte, *supra* note 175, at 4–5.

179 17 U.S.C. § 107(2); *see supra* note 95 and accompanying text.

180 387 F.3d 522 (6th Cir. 2004) (concluding that a computer 'lock-out' code falls outside of the protections of copyright law and the DMCA partly because of the merger doctrine which precludes copyright protection from works where the idea, which is not generally pro-

that Apple's iPhone OS is similar to the lock-out mechanisms in *Lexmark*, the nature of the iPhone OS suggests it deserves little protection.[181] Finally, the author argues that "in order to avoid overly broad copyright protection at the expense of non-infringing uses, the Librarian [of Congress] should find that the incorporation of Apple's [iPhone OS] constitutes fair use."[182]

For the third factor, the amount of the copyrighted work used,[183] Witte admits that virtually all of Apple's software is copied and re-used as part of the jailbreaking process, but he suggests this use "will neither impact the market for the original firmware, nor the iPhone itself."[184]

Discussing the fourth factor, the effect on the market for the copyrighted work,[185] Witte essentially sides with the EFF's view that the iPhone OS has no independent economic value.[186] The author argues that demand for the iPhone device will not decrease if jailbreaking is permitted, and the market will not be harmed as a result.[187]

IV. ANALYSIS

While each side has raised significant concerns regarding whether the Library of Congress should grant the proposed exemption, prior judicial opinions and Library of Congress rulemakings suggest that the proposed exemption will be denied. From a policy perspective, this Note argues such a result may have negative implications for owners of tethered devices, such as the iPhone. More broadly, this Note argues that current interpretations of the DMCA may be a threat to the innovation the law was arguably intended to protect. Regardless, the courts and the Library of Congress have interpreted the Congressional mandate under the DMCA as weighing strongly in favor of copyright holders when it comes to balancing the rights of creators and consumers and the Library is unlikely to exempt the proposed class.

This final section of the paper will discuss potential harms to consumers and Apple and will then review past judicial decisions and Library of Congress rulemakings as a component of an analysis of the legal landscape. Finally, this section will conclude with a brief policy discussion raising concerns about the impact of the DMCA.

---

tectable under copyright, cannot be otherwise separated from the author's expression); *see* Witte, *supra* note 175, at 6–8.

181 *See* Witte, *supra* note 175, at 6–8.

182 *Id.* at 8.

183 17 U.S.C. § 107(3); *see supra* note 95 and accompanying text.

184 Witte, *supra* note 175, at 8–9.

185 17 U.S.C. § 107(4); *see supra* note 95 and accompanying text.

186 *See* Witte, *supra* note 175, at 10.

187 *See id.*

A. *Consumer Harm*

The EFF's proposed exemption comments, as well as other comments submitted to the Library of Congress, demonstrate that some consumers have a strong interest in running legitimately obtained third-party apps on their mobile devices. At the time of the EFF's initial finding in December 2008, it stated an estimated 350,000 consumers had jailbroken their phones and utilized Cydia, an alternative to Apple's App Store that sells licensed apps that may otherwise be unavailable through official channels.[188] While there is no specific data available to show how many jailbroken iPhones are used to run pirated apps, it is clear that there are legitimate pro-copyright reasons for permitting jailbreaking.[189]

Additionally, some individuals submitted comments to the Library of Congress describing the particular legitimate ways they wish to use their mobile devices.[190] For example, Joseph Hall wrote to explain his desire to run a video app that Apple has refused to sell through its App Store.[191] He uses a jailbroken iPhone to make short video clips as a part of his research for a major university.[192] While one could argue he should just buy a video camera or buy the latest version of the iPhone capable of playing video out of the box, it is understandable for a consumer to want to use his lawfully owned device in a convenient manner especially given that the original iPhone is capable of operating as a video camera. Furthermore, it is difficult to argue that this particular use does any harm to Apple's interest. In this instance, Apple has made money from selling the iPhone device to Mr. Hall, and Mr. Hall is better off because he is able to take advantage of the device's capabilities in order to make his research easier. It is likely that consumers like Mr. Hall may have a greater demand for the iPhone device because of the availability of unapproved third-party apps.

---

188 EFF COMMENT, *supra* note 28, at 7 (citing Erica Sadun, *The Story Behind Cydia on the iPhone*, ARS TECHNICA, Oct. 8, 2008, http://arstechnica.com/journals/apple.ars/2008/10/08/the-story-behind-cydia-on-the-iphone)).

189 *See, e.g.*, Sadun, *supra* note 188 (discussing the various apps available through Cydia that cannot be sold through Apple because they offer features which Apple does not permit).

190 *See* Responses to Comments, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, http://www.copyright.gov/1201/2008/responses/index.html (last visited Mar. 17, 2010).

191 Letter from Joseph Lorenzo Hall, Ph.D, Center for Information Technology Policy, to Office of the General Counsel, U.S. Copyright Office (Jan. 30, 2009), *available at* http://www.copyright.gov/1201/2008/responses/joseph-hall-09.pdf.

192 *Id.* While the newer iPhone 3GS model is capable of recording videos out of the box, Apple does not list the original iPhone as capable of recording video. *See* iPhone 3GS Technical Specifications, http://www.apple.com/iphone/specs.html (last visited Mar. 8, 2010); iPhone 3G Technical Specifications, http://www.apple.com/iphone/specs-3g.html (last visited Mar. 8, 2010).

B. *Potential Harm to Apple*

While people, like Mr. Hall, may have a clear and understandable interest in jailbreaking their iPhone devices, Apple posits that its own interests will be adversely impacted if the Library of Congress exempts jailbreaking.[193] As Apple argues, it has a strong interest in maintaining a consistent user experience and in reducing support costs.[194] While the argument that jailbreaking increases support costs makes sense, it is not clear if a court would find a proximate relationship between copyright interests and the harm this places on Apple.

Apple has strong interests in providing a consistent user experience. It markets the iPhone by focusing on the many apps the device can play.[195] Although the iPhone may feel like a full-featured computing device, Apple had to make design choices including balancing the size of the unit, size of the battery, operating speed of the processor, and the amount of volatile high-speed memory (RAM).[196] While consumers may want a small and responsive phone with great battery life, these factors often conflict with each other, leading manufacturers to make compromises. One such compromise on the iPhone is to virtually ban the running of apps in the background.[197] Desktop computer users take for granted the ability to have many programs running simultaneously (multitasking). For example, a consumer may write a paper using a word processing program while running an instant messaging program in the background. Computer users often switch back and forth between these types of applications, however, this capability requires more memory and processing power than if only one application is run at a time. For the iPhone, Apple chose to limit background processing making it impossible to multitask. If a desktop computer worked like this, it would mean

---

193 While completely speculative, it is possible that an exemption may have little real-world impact. Many iPhone owners have jailbroken their phones already, unaware of or despite potential legal consequences. *See* EFF COMMENT at 5 (noting that over 350,000 users had jailbroken their phones as of fall 2008). It may be the case then that an official exemption will lead to minimal change in the demand for jailbreaking. Creators like Apple will likely caution about the risks of these activities and are able to keep many consumers in check by voiding their warranties if they jailbreak. At the same time, many developers may see jailbreaking as an opportunity to develop programs outside of Apple's restrictions on features. These new apps may drive consumer demand for jailbreaking.

194 *See supra* note 136 and accompanying text.

195 *See, e.g.*, Press Release, Apple Inc., App Store Downloads Top 100 Million Worldwide (Sept. 9, 2008), *available at* http://www.apple.com/pr/library/2008/09/09appstore.html.

196 *See, e.g.*, Mark Burgess & Frode Eika Sandnes, *A Promise Theory Approach to Collaborative Power Reduction in a Pervasive Computing Environment*, *in* LECTURE NOTES IN COMPUTER SCIENCE 616 (Aug. 25, 2006), *available at* http://www.springerlink.com/content/t669g12u50r7l008/ (describing the problems stemming from the relationship between battery life and processor usage).

197 *See* Rob Griffiths, *Some Background on Background Processes*, MACWORLD.COM, Jun. 10, 2008, http://www.macworld.com/article/133867/2008/06/backgroundprocesses.html.

consumers would have to save and quit their word processor before opening and signing into their instant messaging client to converse with a colleague.[198]

The iPhone likely has these types of restrictions on multitasking, as well as restrictions on the use of certain apps, because Apple wants to ensure consumers experience great battery life and fast response from the iPhone device and its apps. In order to create this positive user experience, Apple chose to place limits on the iPhone's operations. If jailbreaking were permitted, memory hogging third-party apps or other iPhone OS modifications may increase features with the effect of decreasing battery life or straining the processor in ways that take away from the quick response time Apple intended as part of the positive iPhone experience.[199]

Finally, Apple has a strong interest in reducing app piracy. While jailbreaking on its own does not interfere with the TPMs designed to prevent copying of apps distributed through the App store, jailbreaking is a necessary step on the road to running pirated apps. People like Mr. Hall demonstrate that there are legitimate reasons to allow users to download and run apps from sources other than Apple's App Store.[200] Unfortunately, opening the door to permit developers to distribute their apps outsides of Apple's official channel also means unlocking part of the protections designed to prevent users from running pirated apps, which could hurt developers and may lower overall incentives for app development. Apple's "ecosystem" provides strong incentives for developers to produce apps because it is safe and secure. Owners of iPhones who have not jailbroken their devices have no way to run pirated apps, and these restrictions help to ensure apps are only acquired through Apple's legitimate channel. While this system may reduce iPhone users' choices regarding where to purchase their apps or what types of apps they can use on their iPhone, it also creates strong incentives for the production of copyrighted works (apps). As the volume of apps in-

198 Users of MS-DOS or early versions of Microsoft Windows may be familiar with this scenario.

199 When using an Apple Macintosh computer or a PC running a version of Microsoft Windows, there are times when everything slows down—video playback may appear choppy or scrolling in a web browser may no longer appear smooth. This type of behavior may be the result of using too many programs at once and it likely affects how consumers view their computing experience. It is possible that Apple wished to limit these negative experiences on the iPhone by placing limits on running multiple programs simultaneously. Likely due to these concerns, Google's Android OS has a policy of permitting multi-tasking but with the understanding that the phone may close background applications when the system needs to free up memory or processing time. *See* Peter Bright, *Leaked: WinPhone 7 Series Dev to Use Almost All Managed Code*, ARS TECHNICA, Feb. 19, 2010, http://arstechnica.com/microsoft/news/2010/02/windows-phone-7-series-development-kit-info-leaks.ars.

200 *See* Hall, *supra* note 191 and accompanying text.

creases, the value of the iPhone increases for consumers because each app essentially adds new capabilities or features to the phone. The resulting increased demand for iPhones and its accompanying iPhone OS creates value for Apple because of a higher volume of iPhone sales. Jailbreaking may lessen the incentives that Apple has created for developers to create new apps.

C. *Legal Arguments*

While the concerns of the public and Apple have great importance in this debate, the outcome of the proposed exemption will depend on the law and not on public and private interests directly. In particular, Apple and the EFF have made some questionable claims regarding 17 U.S.C. § 117, fair use, and the likely final outcome for the proposed exemption.

1. Section 117

The EFF and Apple both make questionable claims regarding § 117; however, Apple's argument more closely fits with the court's views in *Krause v. Titleserv, Inc.*[201] While Apple's overall argument may be stronger, it makes a weak argument regarding the ability to negate the § 117(a) adaptation right by contract. Regardless of the outcome of this issue, the EFF fails to demonstrate how jailbreaking could fall within the scope of the § 117(a) adaptation right if Apple's very aim was to prohibit these types of modifications.[202]

In order for § 117 to apply, *Krause* states that while the possessor of the program need not be the original creator or owner of the work, there must be "sufficient incidents of ownership over a copy of the program to be sensibly considered the owner of the copy."[203] In other words, one threshold requirement for § 117 is that the user must own the particular copy of the work at issue. Apple claims that it has contractually limited the adaptation rights of all users.[204] Apple relies on the CONTU Report, which states that copyright owners may elect to contractually prohibit adaptations.[205] Apple points out that § 117 cases extensively cite the CONTU report, but courts have never addressed this issue directly.[206] Further, at least one case suggests in dicta that even where there is a contract, the creator's right to exclude adaptation by contract is not abso-

---

201 402 F.3d 119 (2d Cir. 2005).

202 *See supra* notes 127–29 and accompanying text.

203 *Krause*, 402 F.3d at 124.

204 APPLE COMMENT, *supra* note 120, at 13–14.

205 CONTU Report, *supra* note 127, at 13–14.

206 *See* APPLE COMMENT, *supra* note 120, at 14.

lute.[207] The outcome of Apple's contract negation argument is unclear given the lack of a definitive judicial holding.

While Apple's claims regarding contracting around § 117 might be correct, its arguments regarding the scope of permissible adaptations is more in line with caselaw. Here, the EFF argues:

> The court in *Krause v. Titleserv* also recognized that § 117(a) permits the owner of a copy of a computer program not only to make additional copies, but also to adapt those copies to add new capabilities, so long as the changes do not 'harm the interests of the copyright proprietor.' Where jailbreaking is concerned, the changes to the [iPhone OS] are made solely in order to facilitate the interoperability of the phone with third-party applications, and the resulting modified firmware is used on the phone on which the firmware was originally installed.[208]

The first issue with the EFF's argument is that real harms will result if the Library exempts jailbreaking. Apple has understandable concerns regarding maintaining a consistent and high quality user experience that may be tarnished by processor-hungry programs causing the iPhone to run slowly or significantly reduce the device's battery life. Further, Apple correctly points out that the *Krause* court believed the scope of permissible adaptations depends on the "use envisioned in the creation of the program."[209] In *Krause*, the program at issue was a business records management program.[210] The permitted modifications included making changes to reflect the current business operational needs of the owner of the copy of the program.[211] The iPhone and the jailbreaking adaptation seem significantly different considering that the iPhone was always locked-down to ensure that only Apple-approved code may be executed. Apple designed the iPhone OS with the specific intent of maintaining operational integrity, including through the restrictions on the use of non-App Store apps. If this view of Apple's envisioned use of the iPhone OS is correct, it is hard to imagine that an adaptation which destroys these protections could fall within the scope of adaptations permitted under § 117.

---

207 Foresight Res. Corp. v. Pfortmiller, 719 F. Supp. 1006, 1010 (D. Kan. 1989).

208 EFF COMMENT, *supra* note 28, at 9.

209 APPLE COMMENT, *supra* note 120, at 17 (citing Krause v. Titleserv, Inc., 402 F.3d 119, 129 (2d Cir. 2005)).

210 Krause v. Titleserv, Inc., 402 F.3d 119, 120 (2d Cir. 2005).

211 *Id.*

2. Fair Use

While the EFF makes some strong points in its fair use argument, the DMCA exemption will likely be denied independent of whether the Library of Congress agrees with Apple or the EFF with regard to fair use.[212] Even the EFF and Witte's[213] respective fair use arguments, however, are not ironclad. Both make questionable claims regarding the fourth fair use factor, the effect of the use upon the potential market for or value of the copyrighted work.[214] The EFF argued that the fourth factor favors fair use: "Insofar as smart phone makers do not copy or distribute [the iPhone OS] separately from the smart phones themselves, the jailbreaking activities of individual phone owners cannot harm the market for the phone/[iPhone OS] bundle."[215]

The EFF continues to argue that the iPhone OS has no independent economic value separate from the iPhone.[216] This argument ignores the incentives Apple has created through the many TPMs used on the iPhone in order to provide an environment where it is easy to monetize apps and impossible to run pirated copies. To the extent that the iPhone's value depends on the number and quality of apps available for use, it seems that activities like jailbreaking would decrease incentives to create new apps and that this decrease would lower the value of the iPhone. While the EFF may be correct that some specific consumers, such as Mr. Hall,[217] will be more likely to demand the iPhone if allowed to jailbreak, the aggregate effect of jailbreaking may have deleterious effects on the current incentives to create apps and on the value of the iPhone OS.

3. DMCA

Whether Apple or the EFF are correct in their arguments regarding fair use and § 117, the proposed exemption may still fail because of the wide scope of its applicability. The proposed exemption would apply to smart phones generally and not just the iPhone. Furthermore, virtually all consumers would fall within the class of users permitted to jailbreak. The problem with such a wide scope is that the design of each smart phone may vary substantially, and possibly, the steps necessary for jailbreaking may also compromise otherwise protected software and media. The fact that jailbreaking some devices may potentially compromise

---

212 *See supra* Part III (discussing the likely problems with the scope of the proposed class).

213 *See* Witte, *supra* note 175.

214 17 U.S.C. § 107(4) (2006).

215 EFF COMMENT, *supra* note 28, at 9.

216 *Id.*

217 *See* Hall, *supra* note 191 and accompanying text.

TPMs aimed at preventing the copying of protected media may be a dispositive factor for the Library.[218]

In previous rulings, the Library of Congress has addressed issues analogous to the proposed jailbreaking exemption. Perhaps the strongest and most recent example comes from the 2006 rulemaking. That rulemaking denied a proposed exemption for playing region-coded DVDs.[219] Commercial movies distributed on DVD are classified by geographical region.[220] For example, DVDs purchased in North America are in Region 1 and those sold in China are in Region 6.[221] DVDs and DVD players sold in each region share the same Region code, and DVD players are only supposed to play DVDs for one region. Just as the iPhone will play Apple authorized apps only, a Region 1 DVD player will play DVDs coded for Region 1 only. Also, some movies may be released in one region but not in others.[222] The result of these complications is that American viewers may be unable to watch certain movies that have not been released for Region 1. This restriction on the ability to play the movies that one wants is quite similar to the jailbreaking interest in playing apps of all kinds independent of Apple's approval. The Register of Copyrights denied an exemption for region-coded DVD in part because of a finding that alternatives existed for playing DVDs from other regions, including buying a second DVD player with the desired region code.[223] Additionally, the Register of Copyrights viewed the restriction as an inconvenience and not a harm because of available alternatives.[224] Perhaps the Register of Copyrights will recommend that people like Mr. Hall, who wish to make videos with their iPhones, just buy a video camera or a newer iPhone model instead.[225]

A second analogous use that has not been addressed directly by the Register of Copyrights, but that has been considered in court, is mod chips for video game systems. Mod chips are computer chips which can be soldered to video game systems in order to defeat the copy protection

---

218 2006 RECOMMENDATION, *supra* note 79, at 52.

219 *See id.* at 74.

220 *See id.*

221 *See generally* ROBERT C. BIRD & SUBHASH C. JAIN, THE GLOBAL CHALLENGE OF INTELLECTUAL PROPERTY RIGHTS (2008) (discussing the use of regional codes to prevent the viewing of pirated DVDs).

222 For example, a 2001 Washington Post article noted that "immigrants who want to watch movies from their home, language students and foreign film enthusiasts," are some of the groups that are negatively impacted by the region code system and sometimes resort to the use of banned multiregion DVD players. James C. Luh, *Breaking Down DVD Borders*, WASH. POST, June 1, 2001, http://www.washingtonpost.com/ac2/wp-dyn/A5310-2001May31.

223 2006 RECOMMENDATION, *supra* note 79, at 75.

224 *See id.* at 75–76.

225 *See* Hall, *supra* note 191.

measures.[226] These chips defeat video game system TPMs that block the system from running copied game discs, games intended for a different geographical market (similar to DVD Region Codes), and also unlicensed third-party software. Just as Apple uses TPMs to block the use of non-App Store programs, video game manufacturers such as Sony have used TPMs to ensure only Sony-authorized software can be run on its machines.[227] In *Sony Computer Entertainment America, Inc. v. Filipiak*,[228] the court found an individual liable for distributing mod chips in violation of the DMCA.[229] Because the protections defeated through jailbreaking are similar to those defeated by mod chips, *Filipiak* provides further support for the argument that the proposed jailbreaking exemption will be denied.

4. Policy: Innovation Incentives

While I argue Apple is likely to prevail in its quest to quash the proposed jailbreaking exemption, I do not believe this outcome, which comports with contemporary interpretations of the DMCA, is necessarily the best result for the public. While the iPhone's closed model has attracted consumers and developers in a manner that appears to have raised consumer interest in the smartphone market, it has also arguably hindered the development of valuable disruptive technical innovation.

The goal of the anti-circumvention provisions is in part to ensure that content creators will continue to control the digital distribution of their media (music, movies, software, etc.). According to a U.S. Copyright Office Summary, the anti-circumvention provision and its associated causes of actions, "provide legal protection that the international copyright community deemed critical to the safe and efficient exploitation of works on digital networks."[230] In other words, legislators likely felt the enactment of the DMCA was necessary to protect copyright holders so that they will continue to have incentives to produce new creative works. While such an aim, if achievable, seems laudable, it is ironic that the DMCA can be relied upon to exclude those who wish to create new and innovative software for locked-down devices like the iPhone.[231] In a

---

226 *See* Phillip A. Harris, Jr., *Mod Chips and Homebrew: A Recipe for Their Continued Use in Wake of* Sony v. Divineo, 9 N.C. J.L. & TECH. 113, 115–16 (2007).

227 *See id.*

228 406 F. Supp. 2d 1068 (N.D. Cal. 2005).

229 *Id.* at 1076–77.

230 U.S. COPYRIGHT OFFICE, SUMMARY OF THE DIGITAL MILLENNIUM COPYRIGHT ACT 3 (1998), *available at* http://www.copyright.gov/legislation/dmca.pdf.

231 *See, e.g.*, Roi Carthy, *Tawkon Measures the Radiation Spewing From Your iPhone. No Wonder Apple Doesn't Approve It*, TECHCRUNCH, Mar. 4, 2010, http://techcrunch.com/2010/03/04/tawkon-iphone-radiation (discussing a software company's inability to get Apple's approval for an app which attempts to predict the level of radiation emitted by the phone depending on various factors such as the specific model and location of the device).

closed environment, developers may not be able to release highly desirable software if the controlling party, in this case Apple, refuses to give them permission. While a closed model, may offer certain protections and conveniences, it may be bad for innovation, since the controlling party can serve as a gatekeeper, and the consumer's interests are not necessarily aligned with companies like Apple.[232]

While the DMCA provides legal muscle in support of Apple's controlled iPhone business model, it does so at the expense of other developers who might, in the absence of a gatekeeper like Apple, be incentivized to produce tomorrow's innovations.

CONCLUSION

It is unfortunate that some iPhone users are unable to run certain apps because Apple has chosen not to distribute them. From the standpoint of consumers, the iPhone would be even better if a fully-featured Skype App were available. Furthermore, as discussed just prior to this final section, permitting a jailbreaking exemption might be a net societal benefit. Perhaps the problems of app piracy are not as substantial as Apple suspects, and a jailbreaking exemption will make Apple, developers, and iPhone consumers all better off. While the EFF believes this is the correct way to interpret the proposed exemption, it ignores the draconian all or nothing Congressional mandate under the DMCA. The world of black box[233] technologies no longer exists as imagined when DMCA was enacted. In its place is a world filled with software-restricting software. Organizations like the EFF devote substantial resources to fighting for DMCA exemptions in an attempt to bring balance to copyright law. While such fights may be commendable, the underlying problem, if there is one, is with the DMCA itself.

---

232 Consider the Skype app discussed *supra* notes 1–10 and accompanying text. While consumers would likely prefer to make Skype phone calls using their mobile carrier's data network, ultimately Apple, not Skype or iPhone users, decides whether to allow the distribution of a more full-featured version of the app.

233 *See supra* note 75 and accompanying text.