Sour Apple: The Case For iPhone Jailbreaking
A Study of the DMCA Anti-Circumvention Provision

Anthony M. Brown
Southern University Law Center
2nd place, SULC, ASCAP Nathan Burkan Memorial Competition

Table of Contents

Introduction and Overview 2

Technical Background of the iPhone and Jailbreaking 6

The Argument for Jailbreaking 7

The Argument Against Jailbreaking 9

Reverse Engineering 10

DMCA Litigation 12

Conclusions 19

Introduction and Overview

On June 29, 2007, Apple Inc. released the iPhone, a so-called "smart phone" to much fanfare and excitement.[1] Despite being disproportionally more expensive than its competitors, it sold several million units within a few months of its release.[2] However, the phone was widely criticized for lacking basic features that other smart phones had. It was not possible for the home user or third party developers to expand the phone's functionality. Shortly after its release, a group of skilled computer hobbyists discovered how to modify the phone's functionality, and developed their own software development kit, or SDK, to allow third parties to add functionality to the phone.[3] Modifying the phone's functionality and adding these particular third party programs require the phone's user to "jailbreak" the phone, which requires them to use a third party program, to circumvent the various protection methods put in place on the phone to prevent end-users from modifying its functionality.[4] There are various methods of jailbreaking, but all of the methods require the user to modify the iPhone's bootloader, which is protected by numerous software verification checks, to allow a modified version of Apple's iPhone

---

[1] Press Release, Apple Inc., iPhone Premieres This Friday Night at Apple Retail Stores (Jun. 28, 2007), http://www.apple.com/pr/library/2007/06/28iphone.html.
[2] David Chartier, *Apple Sells 1 millionth iPhone, Steve Ballmer not available for comment*, ARS TECHNICA, Sep. 10, 2007, http://arstechnica.com/apple/news/2007/09/apple-sells-1-millionth-iphone-steve-ballmer-not-available-for-comment.ars.
[3] Don Reisinger, *Jailbreak: the iPhone hacking story*, TECHRADAR.COM, Nov. 9, 2007, http://www.techradar.com/news/audio/portable-audio/jailbreak-the-iphone-hacking-story-153739.
[4] The term "jailbreak" originates from the UNIX command "chroot" which changes a computer's apparent operating directory and prevents the user from leaving that directory, which is commonly referred to as a "chroot jail".

operating system to be placed onto the device.[5] This modified version of the operating system is created by the individual user, on his or her own computer, using legitimately licensed and obtained versions of Apple's own software.[6] After jailbreaking became so commonplace that demonstration iPhones in Apple's own stores were being jailbroken by hobbyists, Apple announced its own SDK for the iPhone and a means to control third-party software distribution, known as the "App Store".[7] In order for a third-party developer to distribute their programs for the iPhone, they must first pay a $99 per year fee to Apple, they must agree to sell their program through Apple's "App Store", and they must agree to share thirty percent of the revenue generated by the program's sale, along with agreeing to provide refunds, making up the thirty percent cut given to Apple by themselves, to unsatisfied users if the program is to be sold on the store.[8] Additionally, Apple must approve every program that is to be listed on the "App Store", and the programs must meet a vague set of guidelines to be approved for listing in the store.[9] Despite the changes in functionality that Apple has made to the phone, jailbreaking is still widespread, used by a significant portion of the iPhone's user base, and utilized by third-

---

[5] Comments of the Electronic Frontier Foundation, to Library of Congress, Copyright Office, In the matter of exemption to prohibition on circumvention of copyright protection systems for access control technologies, (2009), *available at* http://www.copyright.gov/1201/2008/responses/electronic-frontier-foundation-50.pdf.
[6] Seth Schoen, *A Technical Overview of Smart Phone Jailbreaking and Unlocking*, Feb. 2, 2009, *available at* http://www.eff.org/files/filenode/dmca_2009/EFF2009replycomment_0.pdf.
[7] Press Release, Apple Inc., Apple Announces iPhone 2.0 Software Beta (Mar. 6, 2008), http://www.apple.com/pr/library/2008/03/06iphone.html.
[8] Candace Lombardi, *Apple refund clause: Bad for developers?*, NEWS.COM, Mar. 26, 2009, http://news.cnet.com/apple-refund-clause-bad-for-developers/.
[9] Other phone manufacturers and phone platform developers have adopted or have looked into this business model, including Nokia, Google (with their "Android" mobile platform), and Microsoft.

party developers in order to get around the limitations on development put into place by Apple.[10]

Congress passed the Digital Millennium Copyright Act, or DMCA, on October 12th, 1998; it was passed by a voice vote in the House, and unanimously in the Senate.[11] Among the many provisions that the DMCA added to Title 17 of the U.S. Code was §1201(a), a prohibition on circumventing technological measures that control copyright-protected works; this provision is better known as the "anti-circumvention provision." 17 U.S.C. §1201(a)(2)(A) provides that. . . .

> "[N]o person shall manufacture, import, offer to the public, or otherwise traffic in any technology, product, service, device, component or part thereof that is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title."

There are a few statutory exemptions to the anti-circumvention provision. §1201(f) provides some exemptions for the purposes of reverse engineering to achieve interoperability of an independently created computer program, while §1201(g) provides an exemption for encryption research, to allow for security researchers to identify flaws and vulnerabilities of encryption technologies. Finally, §1201(j) allows users to perform security testing on a computer, computer network, or computer system for the sole purpose of good faith testing, investigation, or correcting a security flaw found on that computer, computer system, or computer network.

In addition to the statutory exemptions to the anti-circumvention provision, §1201(a)(1)(E)(2) provides that the Library of Congress may issue its own exemptions to the anti-circumvention provision for whatever they deem necessary. The Library of

---

[10] Electronic Frontier Foundation, *supra* note 5.
[11] 144 CONG. REC. S4894 (daily ed. May 14, 1998) (Roll Call Vote No. 137).

Congress has done so previously, issuing exemptions for unlocking cell phones to work on any network,[12] allowing protected e-books to be read aloud for the blind,[13] and for permitting users to circumvent computer programs and video games which are distributed in formats which are obsolete.[14]

Every three years, ordinary citizens, corporations, and interest groups are permitted to petition the Copyright Office to recommend further exemptions to the anti-circumvention provision. One of the leading interest groups to propose exemptions to provision is the Electronic Frontier Foundation (or "EFF") – a non-profit group based out of San Francisco, California whose mission is to "beat back bad legislation" related to electronic rights.[15] In the most recent rule-making session, the EFF has recently proposed an exemption to the Copyright Office to allow users to "jailbreak" their "smart phones", such as Apple's iPhone and Google's "Android" platform. Apple is adamantly opposed to this proposed exemption. . . .

> "[B]ecause it 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."[16]

Apple's position, while understandable, is for naught, as there are numerous flaws in their position, including the fact that courts have long recognized the end-user's

---

[12] Exemption to prohibition against circumvention, 37 C.F.R. § 201.40 (2006).
[13] *See id.*
[14] *See id.*
[15] ABOUT EFF, http://www.eff.org/about (last visited May 12, 2009).
[16] Responsive Comment of Apple Inc., to Library of Congress, Copyright Office, In the matter of exemption to prohibition on circumvention of copyright protection systems for access control technologies, (2009), *available at* http://www.copyright.gov/1201/2008/responses/apple-inc-31.pdf [hereinafter Apple Exemption].

ability to reverse engineer a software and hardware product for the purposes of interoperability, and the holdings in *Lexmark Int'l v. Static Control Components*, *Universal v. Reimerdes*, and *Chamberlain Group Inc. v. Skylink Inc.* are applicable to iPhone jailbreaking, as they are analogous situations.

Technical Background of the iPhone and Jailbreaking

The iPhone is comprised of two distinct computers in the handset – a central processing unit (or CPU), which contains a modified version Apple's OS X operating system, and a baseband, which controls the phone and networking aspects of the phone.[17] The CPU restricts users from running unapproved applications, and has a "chain of trust" built in to prevent users from substituting their own software on the phone – whenever the phone is turned on or rebooted, a number of components do "signature checks" at four stages to make sure nothing has been modified and will refuse to boot the phone if any signature check fails; however, no such signature check is done at the first stage of the booting process.[18] This allows for patched versions of the operating system to be substituted. Using software developed by hobbyist groups, the iPhone owner can load "patched" versions of the iPhone operating system, created on their own computer from legitimately obtained and licensed software distributed to every iPhone owner.[19] However, to create the patched version of the operating system, the user must circumvent, as envisioned under 1201(a), encryption placed on copies of the iPhone

---

[17] Schoen, *supra* note 3.
[18] *See id.*
[19] *See id.*

operating system; this encryption method is not original, rather it is a widely used standard form of encryption, RSA.[20]

The Argument for Jailbreaking

There are several reasons why an end-user, hobbyist, or developer would want to "jailbreak" their iPhone. Initially, when the iPhone was released, and Apple did not provide any sort of way for a user to install third party applications, but they did allow developers to create "Web Apps" which users could access via the phone's built-in web browser. These "Web Apps" were extremely limited in functionality.[21] When jailbreaking was developed, it allowed the user to add on to the functionality of the phone – developers could create programs that could run natively on the phone and do much more than was possible using the phone's web browser. However, this point became moot when Apple released the first major update to the phone's operating system, iPhone OS 2.0 – this was the update that added support for the "App Store" and allowed users to install third party applications, approved by Apple, that could run natively on the phone.[22]

But, through the "legitimate" method of running and installing applications through the "App Store", Apple controls all of the programs that can be installed and operated on the phone, and they also control which applications can be listed on the "App Store".[23] Additionally, Apple has added a "kill switch" the phone, which can be invoked

---

[20] *See id.*
[21] iPhone web app development has its limitations, http://hunter.pairsite.com/blogs/blog20070820.html (Aug. 20, 2007).
[22] Press Release, Apple Inc., Apple Introduces the New iPhone 3G (June 9, 2008), http://www.apple.com/pr/library/2008/06/09iphone.html.
[23] Rob Pegoraro, *Apple Irks iPhone Developers With App Store Restrictions*, WASHINGTONPOST VOICES, Sep. 29, 2008,

remotely to disable any application at any time if it poses a security concern, or if they simply do not like it.[24] Apple has set out a bare set of guidelines as to what can be sold or put up for download[25] on the "App Store" – described simply as "malicious", "illegal", "unforeseen", "porn", "privacy", and "bandwidth hog" in Apple's own presentation on what cannot be included on the store.[26] However, it has been shown in the year or so since the "App Store" first opened that these overly broad categories of programs that will not be included on the store are not the only types of programs being excluded. Programs have been rejected for "competing" with Apple's own applications,[27] for having "dirty" words in them (despite the fact that Apple's own iTunes music store sells the same music, by the same artist, that must simply be branded with a "parental advisory" in order to be listed),[28] for being in poor taste[29], for disparaging public figures[30], and for absolutely no stated reason at all.[31] Apple has gone as far as claiming

---

http://voices.washingtonpost.com/fasterforward/2008/09/apple_irks_iphone_developers_w.html

[24] Tom Krazit, *Much ado about the iPhone's kill switch*, NEWS.COM, Aug. 7, 2008, http://news.cnet.com/8301-13579_3-10010070-37.html

[25] Not all programs listed on the App Store cost money – they must be listed there, however, for a user to be able to install them on his or her iPhone.

[26] Posting of Ryan Block to Engadget, http://www.engadget.com (Mar. 6, 2008, 12:51 CST).

[27] Posting of Robert Palmer to The Unofficial Apple Weblog, http://www.tuaw.com/ (Sep. 12, 2008, 20:18 CST).

[28] Posting of Timothy M. O'Brien to O'Reilly's Radar, http://radar.oreilly.com/ (May 5, 2009, 14:39 CST).

[29] Ryan Kim, *Baby-Shaking App Raises Questions About Apple*, S.F. CHRON., Apr. 24, 2009, at C-1.

[30] Posting of Brian X. Chen to Gadget Lab, http://www.wired.com/gadgetlab/ (Feb. 9, 2009, 14:30 CST).

[31] iPhone Application Graveyard, http://boredzo.org/killed-iphone-apps/.

that application rejection notices were covered under a "Non-Disclosure Agreement", possibly in an effort to subvert any bad press about the rejections.[32]

Jailbreaking allows developers to create these programs that end-users would want, but would not be allowed in the "App Store" for one reason or another, or could not even be developed with the official SDK.[33] Some examples of these programs include instant messaging applications that provide background notification (a feature that Apple does not wish to provide due to concerns about the phone's battery life)[34], cellular network unlocking applications[35], and programs that will locate the phone for its owner in the event that it is lost or stolen[36].

The Argument Against Jailbreaking

Apple wants to control access to their platform for a wide variety of reasons – to secure the platform against malicious applications[37], for profit, to protect the mobile carriers that provide iPhone service, and to protect themselves against any disadvantageous position that unapproved applications might put them in; there is certainly nothing stopping them from controlling the platform. In each new iPhone OS

---

[32] Thom Holwerda, *Apple Adds NDA to App Store Rejection Notices*, OS NEWS, Sep. 24, 2008, http://www.osnews.com/story/20321/Apple_Adds_NDA_to_App_Store_Rejection_Notices.

[33] Posting by Jonathan Zdiarski to O'Reilly OnLamp, http://www.onlamp.com (Mar. 25, 2008).

[34] Background notifications are not currently supported in the most current public version of the iPhone software development kit.

[35] Posting of Brian Lam to Gizmodo, http://www.gizmodo.com/ (Sep. 15, 2007, 22:45 CST).

[36] iLocalis, http://www.ilocalis.com.

[37] *Apple Exemption*, *supra* note 16.

software release, they have come up with ways to "kill" jailbroken iPhones.[38] Additionally, it could be said that Apple does not want to open themselves up to unnecessary expenses by providing technical support to users who run unapproved applications and unintentionally break their iPhones.[39]

By allowing a circumvention exemption for jailbreaking, it could potentially cost Apple a lot of money in additional support costs, in addition to more costs for cell phone providers, if unapproved applications consume an abnormal amount of data. Additionally, allowing users to jailbreak their iPhones would lead to a reduced user-experience, and could potentially tarnish the brand image of the iPhone; Apple has had bad experiences in the past in regards to losing control over its own platforms – the Mac and the Lisa, back in the 1980s.[40]

Reverse Engineering

Courts in the United States and many other countries around the world have long held that it is legal to reverse engineer artifacts, processes, hardware and software systems, even when they are protected by trade secrets, as long as the reverse engineering is done legitimately.[41] Reverse engineering of computer software and hardware is legal, provided it is done for the purposes of interoperability. But the iPhone licensing

---

[38] Posting of Kevin to iPhone Footprint, http://www.iphonefootprint.com/ (Jan. 29, 2009).
[39] iPhone Service: Frequently Asked Questions, http://www.apple.com/support/iphone/service/faq/ (last visited May 13, 2009).
[40] Prince McLean, *Jailbreak Stores Plot To Plunder iPhone App Revenue*, APPLE INSIDER, Mar. 9, 2009, http://www.appleinsider.com/articles/09/03/09/jailbreak_stores_plot_to_plunder_iphone_app_revenue.html.
[41] The Supreme Court has addressed the concept of reverse engineering in both Kewanee Oil Co. v. Bicron Corp. (416 U.S. 470) and Bonito Boats v. Thunder Craft (489 U.S. 141).

agreement contains provisions that prohibit the end-user from reverse engineering the phone or the software it contains.[42] Copyrighted software contains both copyrighted and unprotected (or functional) elements.[43] When a programmer or an engineer wishes to design a product that must be compatible with a copyrighted product must "reverse engineer" the copyrighted product to gain access to the functional elements of the copyrighted product.[44] Where disassembly is the only way to gain access to the ideas and functional elements embodied in a copyrighted computer program, and where there is a legitimate reason for seeking such access, disassembly is a fair use of the copyrighted work, as a matter of law.[45]

Here, hobbyists and end-users are reverse engineering the functional elements of the iPhone's copyrighted hardware and software. By doing so, they have developed their own SDK called the "iPhone open source tool chain".[46] The tool chain was completely generated by third-parties, is not subject to a restrictive licensing agreement, does not cost the developer any money to use, and can work on any platform, unlike the official SDK that only works on Apple's own hardware and software – potentially requiring developers to make a costly investment in new hardware and software just to develop for a limited platform such as the iPhone. Using this mode of software development, generated by reverse engineering the iPhone's hardware and software, hobbyists and

---

[42] iPhone Software License Agreement (Sep. 2007), http://images.apple.com/legal/sla/docs/iphone.pdf.
[43] Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510, 1520 (9th Cir. 1992).
[44] Andrew Johnson-Laird, Software Reverse Engineering in the Real World, 19 U. Dayton L.Rev. 843, 845-46 (1994).
[45] *See Sega Enters. Ltd.*, 977 F.2d at 1527-28.
[46] Posting of Tim O'Reilly to O'Reilly Radar, http://radar.oreilly.com/ (Apr. 2, 2008, 11:31 CST).

users have developed numerous applications, which would never be allowed in the App Store due to the store's arbitrary listing requirements, such as applications that provide turn-by-turn GPS directions,[47] internet tethering for laptops,[48] video recording[49], and feature add-ons, such as language packs, to allow more accessibility to users around the world.

It should be noted, however, that with iPhone jailbreaking, the additional element of circumvention is thrown in. It is impossible to disassemble the copyrighted software of the iPhone's operating system to allow such un-approved applications developed with the open source tool chain to run without first circumventing the various signature checks on the iPhone's bootloader, and without also circumventing the encryption placed on the phone's operating system image. However, the anti-circumvention and trafficking provision already provides the following exemption for reverse engineering:

> [A] person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.[50]

DMCA Litigation

The DMCA's anti-circumvention provision has only been litigated a handful of times; there are three major cases: *Chamberlain v. Skylink*, *Lexmark Int'l v. Static*

---

[47] Posting of John Herrman to Gizmodo, http://www.gizmodo.com/ (Feb. 11, 2009, 5:13 CST).
[48] Posting of Dieter Bohn to The iPhone Blog, http://www.theiphoneblog.com/ (Oct. 16, 2008, 12:10 CST).
[49] Cycorder, http://cydia.saurik.com/info/cycorder/.
[50] 17 U.S.C. § 1201(f).

Control Components, and *Universal v. Reimerdes*. The *Reimerdes* case was one of the first cases concerning the DMCA's anti-circumvention provision. In that case, the defendants initially distributed binaries and the human-readable source code to DeCSS, a program which circumvented protections found on every commercially available DVD, which prevent copying and viewing on unlicensed players.[51] After a preliminary injunction was issued, the defendants no longer provided the software personally, but added hyperlinks on their website, leading to third party websites, so visitors could still find the circumvention software.[52] While most of the *Reimerdes* case concerned the "trafficking" aspect of a circumvention method, the court in that case did address some questions concerning the possible legality of using and creating such circumvention methods. In that case, the court held that the DMCA's anti-circumvention provision is not unconstitutional under the First Amendment to the Constitution[53], as the DMCA's anti-circumvention provision is a "content neutral" law.[54] In its reasoning, the court equates the anti-circumvention provision and its laws against trafficking such devices to laws against possessing burglar tools, stating that the reason Congress enacted this portion of the DMCA. . . .

> "[H]ad nothing to do with suppressing particular ideas of computer programmers and everything to do with functionality-with preventing people from circumventing technological access control measures-just as laws prohibiting the possession of burglar tools have nothing to do with preventing people from expressing themselves by accumulating what to them may be attractive assortments of implements and everything to do with preventing burglaries. Rather, it is focused squarely upon the effect of the distribution of the functional capability that the code provides. Any impact on the dissemination of

---

[51] Universal City Studios, Inc. v. Reimerdes, 111 F.Supp.2d 294, 309 (S.D.N.Y. 2000).
[52] *Id.* at 312.
[53] Computer code is protected speech under the 1st amendment.
[54] *Id.* at 329

> programmers' ideas is purely incidental to the overriding concerns of promoting the distribution of copyrighted works in digital form while at the same time protecting those works from piracy and other violations of the exclusive rights of copyright holders."[55]

The holding in *Reimerdes* is not very promising for the jailbreaking crowd. While some scholars agree that if an end-user was prosecuted for using DeCSS, they could likely argue a fair use copying of a DVD, an analogous argument for the iPhone could not be made. There is no software being copied in the case of an iPhone jailbreak, besides the software the user is legally entitled to download from Apple's own website – the software's encryption is just being circumvented and it is being used in a way that the author of the work, Apple, never intended.

In the *Chamberlain* case, the DMCA's anti-circumvention and anti-trafficking provision was once again at issue, however, this time was the first time a court actually discussed the enforceability of the provision on grounds other than constitutional ones. The plaintiff was a manufacturer of garage door opening devices, while the defendant provided a remote control that could work with any garage door-opening device, including the plaintiff's. The plaintiff's device had a special "rolling code" system that was not designed for anti-competitive purposes; rather it was designed as a security measure to keep possible intruders from picking up the garage door opener's activation code over the air and using it for more nefarious purposes later on.[56] The defendant reverse engineered the plaintiff's system to provide a universal remote control for garage door openers; the plaintiff claimed this reverse engineering was in violation of the

---

[55] *Id.* at 328.
[56] Chamberlain Group Inc. v. Skylink Technologies, Inc. 381 F.3d 1178, 1183 (Fed. Cir. 2004).

DMCA's anti-circumvention provision, alleging that the defendant circumvented "technical measures" found in the original remotes.[57]

In that case, the court held for the defendant for several reasons. In its opinion, the court pointed out that when the homeowner purchases a garage door opener, they have the right to use it to access his or her own garage, and can do anything that they like for it.[58] There is no licensing agreement, terms of service, or anything of the sort included with the garage door opener – just its instruction manual, if even that. This is unlike the iPhone, which has a licensing agreement that the end-user must first agree to before they can use it; however, as previously discussed, even with the presence of such a prohibition against reverse engineering in a license agreement, it still is permissible for a user to reverse engineer the functional elements of a copyrighted work for the purposes of interoperability.[59] Even so, if a user purchases an iPhone used from a second hand source, or if they jailbreak their iPhone prior to its activation, they may never agree to, see, or even know about the existence of the iPhone software license agreement, as users can bypass the phone's standard activation process in which they are presented with the license agreement, by jailbreaking their phone.[60]

Additionally, the court in *Chamberlain* also states that the DMCA's anti-circumvention provision does not establish a new property right, rather it establishes a

---

[57] *Id.* at 1183.
[58] *Id.* at 1187.
[59] *See* cases cited *supra* note 41.
[60] Xeni Jardin, *iPhone: DVD Jon claims to activate without ATT… T-Mobile for Europe?*, BOINGBOING (Jul. 3, 2007), http://www.boingboing.net/2007/07/03/iphone-dvd-jon-claim.html.

new cause of action for liability.[61] The court discusses what is needed in order to pursue that cause of action; specifically, a plaintiff has the burden of proving that the defendant's circumvention was unauthorized, while the defendant must prove authorized copying.[62]

Finally, the *Lexmark* case is probably the most applicable to the situation of iPhone jailbreaking. In *Lexmark*, the plaintiff was the manufacturer of printers and their toner & ink cartridges. In order to save money for itself and its customers, the plaintiff began offering a program where they would offer cheaper, remanufactured toner cartridges to their customers; the customers would be obligated to return these cartridges when they were out of toner. To "force" the customer to return the cartridges, the plaintiff designed a chip that contained a 55-byte computer program; this program had some originality, as it contained a computer representation of the plaintiff's stock ticker symbol, but functionally speaking, it would calculate how much toner was in the cartridge and would determine if the cartridge was supposed to be empty by that point in time – the program would not allow the cartridge to function after that point, even if it had been refilled, or still contained toner within the cartridge.[63] The defendant in that case reverse engineered the security chip and released its own chip to be used in its remanufactured printer cartridges, and to be sold to cartridge remanufacturers so that they could refill these cartridges. The defendant included a copy of the 55-byte computer program authored by the plaintiff in its chip; the defendant claimed this was a lock-out

---

[61] *Id.* at 1192.
[62] *Id.* at 1193.
[63] Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 529 (6th Cir. 2004).

code, and was thus a functional element, and not protectable under copyright law.[64] The district court ruled in favor of the plaintiffs, ruling on three points – first, the defendant's chip is indeed a copyright violation, because the plaintiff's chip is not a "lock out code" that they are entitled to copy under the DMCA, because the program could be rewritten and expressed in several different ways, and therefore had enough creativity to qualify for copyright protection[65]; second, that the defendant's computer chip did indeed circumvent the plaintiff's authentication sequence, and the reverse engineering exemption did not apply, because it only applies to independently created computer programs for the purposes of interoperability, not already existing programs such as the one that the defendant had copied; and third, the defendant could have not bypassed the plaintiff's security method without using the plaintiff's copyrighted program, and infringement, even if innocent, is still infringement.[66]

The appeals court in *Lexmark* decided differently, however, ruling in favor of the defendant. The majority opinion in the appellate case differed from the district level in two distinct ways – first, it held that the authentication sequence was indeed a lock-out code, and was therefore precluded from receiving copyright protection due to the sequence being a functional element[67]; second, it held that on the DMCA claims, the plaintiff's authentication chip did not "control access" to the printer's program, rather, the purchase of the printer itself allowed access to the program.[68]

---

[64] Lexmark Int'l, Inc. v. Static Control Components, Inc., 253 F.Supp.2d. 943, 950 (E.D. Ky. 2003).
[65] *Id.* at 964.
[66] *Id.* at 959.
[67] *See Lexmark Int'l, Inc.*, 387 F.3d at 542.
[68] *Id.* at 546.

The first distinction that the appellate court makes is certainly applicable to iPhone jailbreaking. Users who wish to jailbreak their iPhones must circumvent two things – the various signature checks in the power up process, and the encryption placed on the iPhone OS disk image. Both of these could be considered lock out codes – the encryption on the OS disk image is simply a key that can be determined with little effort by hobbyists, and has absolutely no creativity to it – it is just a key made of random numbers, characters, and letters. On top of that, the signature check used on the iPhone's bootloader may not even be considered a method of encryption that could be circumvented as envisioned under the anti-circumvention provision. Rather, it is simply a set of verifications done to assure the integrity of the software. Additionally, nothing is being circumvented if the signature check has a figurative "hole" in it; rather than using the law to pursue their ends, Apple should fix the "hole" in future releases of its iPhone platform, and have done so with recent releases of the iPod touch, which uses the same iPhone platform and software.

Notably, Judge Gilbert Stroud Merritt, Jr. of the sixth circuit agreed with the outcome of this case, and issued a somewhat meaningful concurring opinion that went a bit further, saying:

> [O]ur holding should not be limited to the narrow facts surrounding either the Toner Loading Program or the Printer Engine Program. We should make clear that in the future companies like Lexmark cannot use the DMCA in conjunction with copyright law to create monopolies of manufacturer goods for themselves . . . [69]

With this case, it looks as though Apple is doing exactly what Judge Merritt feared – a company is using the DMCA in conjunction with copyright law to create a

---

[69] *Id.* at 551-52 (Merritt, J., concurring).

monopoly on goods. Here, however, the goods are not goods in the physical sense, manufactured by the corporation, as they were in *Lexmark*, and they're not even goods manufactured by Apple – it is Apple's hold on the distribution method for goods manufactured by developers.

Conclusions

In conclusion, a new exemption to the anti-circumvention provision of the DMCA, while useful and concrete, would not be necessary to protect end-users and hobbyists from prosecution for jailbreaking their iPhones. The principals, which have long been available, and have allowed users to reverse engineer their computer hardware and software that they lawfully own, along with the statutory exemptions to the anti-circumvention provision regarding reverse engineering, should protect end-users, hobbyists, and developers from needless prosecution if they decide to jailbreak their iPhone or develop software that Apple would not approve for distribution in the "App Store".

Finally, while there is little litigation on the subject of the anti-circumvention provision, it seems to be mostly positive for users who wish to jailbreak their iPhones. While *Reimerdes* is not very promising for the jailbreaking cause, it has been superseded and expanded upon in *Chamberlain* and *Lexmark*. *Lexmark* is particularly promising for the jailbreaking cause, as the court took the time to discuss lock-out codes and their applicability in terms of copyright law and the DMCA. Additionally, through Judge Merritt's concurring opinion, it shows that courts are not going to look favorably towards companies who try to use the anti-circumvention provision for monopolistic gains.

Certification

I, Anthony Michael Brown, certify that I have read the Rules Governing the Competition and agree to comply in all respects with those Rules.

_____

Anthony Michael Brown