

# IPHONE JAILBREAKING UNDER THE DMCA: TOWARDS A FUNCTIONALIST APPROACH IN ANTI- CIRCUMVENTION

*Michael K. Cheng*

## I. INTRODUCTION

Over the last ten years, the Smartphone has quickly emerged from technological obscurity to industry standard-bearer.<sup>1</sup> With close to twenty percent of all mobile phone sales expected to be Smartphones by 2013, the growth of the Smartphone market has considerably altered the global telecommunications landscape.<sup>2</sup> In particular, the popularity of Smartphones has created a new type of vendor-consumer lock-in.

A lock-in is a type of relationship where consumers “are dependent on a single manufacturer or supplier for some product (i.e., a good or service) and cannot move to another vendor without substantial costs.”<sup>3</sup> In the United States, most mobile phone users are subject to contractual and technological carrier lock-ins that prevent or discourage usage with unauthorized wireless providers.<sup>4</sup> Buying a mobile phone from a major U.S. carrier will typically require the user to enter into a one or two-year contract with the carrier. The carrier also restricts usage of the device itself through technical measures and

---

© 2010 Michael K. Cheng.

1. While there is no industry definition of what a Smartphone is, the term generally refers to a mobile phone with advanced features typical of those found in personal computers. See Jake Swearingen, *Smartphones gobbling up ever more market share*, VENTUREBEAT, Sep. 10, 2008, <http://venturebeat.com/2008/09/10/smartphones-gobbling-up-ever-more-market-share/>. See generally DELOITTE.COM, TELECOMMUNICATIONS PREDICTIONS: TMT TRENDS (2009), available at [http://www.deloitte.com/dtt/cda/doc/content/dtt\\_2009\\_predictions\\_technology\(1\).pdf](http://www.deloitte.com/dtt/cda/doc/content/dtt_2009_predictions_technology(1).pdf) (last visited Jan. 29, 2010).

2. See RESEARCHANDMARKETS.COM, SMARTPHONE FORECAST - OPERATOR STRATEGIES WILL FUEL GROWTH IN EMERGING MARKETS (2009), available at <http://www.researchandmarkets.com/reports/1187813>. See generally Jamie Lendino, *Smartphone 101*, PC TODAY, Feb. 2006, at 32, available at <http://www.pctoday.com/Editorial/article.asp?article=articles/2006/t0402/12t02/12t02.asp&guid=%3E>.

3. Linux Information Project, Vendor Lock-in Definition, [http://www.linfo.org/vendor\\_lockin.html](http://www.linfo.org/vendor_lockin.html) (last visited Jan. 29, 2010). See generally Alan Beggs and Paul Klemperer, *Multi-Period Competition with Switching Costs*, 60 ECONOMETRICA 651 (1992) (discussing the interplay between market duopolies, new entrants and switching costs).

4. See *Hearing on the Consumer Wireless Experience Before the S. Comm. on Commerce, Sci., and Transportation*, 111th Cong. (2009) (testimony of Rob Frieden, Professor of Telecommunications and Law, Penn State University) [hereinafter Frieden].

end-user license agreements. In recent years, due to the increasing sophistication of Smartphone capabilities and the rapidly maturing market for mobile applications, the industry has witnessed the rise of a new type of lock-in that ties users into the application store (app store) of the handheld manufacturer.<sup>5</sup>

Carrier and application store lock-ins permit wireless providers and mobile phone manufacturers to sell Smartphones at a substantial up-front discount and recoup the difference through wireless service fees and app store sales.<sup>6</sup> Carrier lock-ins bind users to the carrier's wireless service unless users are willing to pay for the service costs and early termination fees incurred upon breach of the wireless agreement.<sup>7</sup> Regardless of whether consumers actually subscribe for the full term of service, wireless providers receive compensation for providing the initial discount of the handset. Unlike carrier lock-ins, which affirmatively binds users to a specific wireless service, application lock-ins seek to prevent or restrict a user's ability to install new applications on the device. In contrast, handset manufacturers have no comparable remedy for breach of its lock-in regimes and may not be able to even detect it.<sup>8</sup> As a result, manufacturers must rely on technological protection measures (TPMs) to prevent alterations to their hardware and software devices in order to preserve their app store market downstream.<sup>9</sup>

To further protect their app store lock-in regimes, manufacturers have argued that disabling or altering handset TPMs are prohibited as acts of illegal circumvention under the Digital Millennium Copyright Act (DMCA).<sup>10</sup> Specifically, § 1201 of the DMCA prohibits the circumvention of any technological measure that "effectively controls access" to a copyrighted work.<sup>11</sup> Section 1201 also provides for the creation of exemptions to the ban on circumvention through a rulemaking process administered by the

---

5. Jenna Wortham, *Apple's Game Changer, Downloading Now*, N.Y. TIMES, Dec. 6, 2009, at BU1; *see, e.g.*, Apple App Store, Apple, Inc., <http://www.apple.com/iphone/apps-for-iphone/> (last visited Jan. 29, 2010); *see also* Freiden, *supra* note 4, at 3.

6. *See* Frieden, *supra* note 4, at 4.

7. *Id.* *See also* Michael L. Katz and Carl Shapiro, *Network Externalities, Competition, and Compatibility*, 75 THE AMERICAN ECONOMIC REVIEW 424 (1985).

8. *See* Dan L. Burk, *Anticircumvention Misuse*, 50 UCLA L. REV. 1095, 1133 (2003).

9. *See id.*

10. *See, e.g.*, Response of Apple Inc. to Questions Submitted by the Copyright Office Concerning Exemptions 5A and 11A (Class #1), In re Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Jun. 23, 2009, *available at* [http://www.eff.org/files/filenode/dmca\\_2009/apple%27s-response-to-copyright-office-questions-of-6-23-09.pdf](http://www.eff.org/files/filenode/dmca_2009/apple%27s-response-to-copyright-office-questions-of-6-23-09.pdf).

11. 17 U.S.C. § 1201(a)(1)(A) (2006).

Librarian of Congress.<sup>12</sup> In February of 2009, the Electronic Frontier Foundation filed a request with the Library of Congress to exempt the circumvention of TPMs for purposes of installing applications from sources not designated by the manufacturer, also known as “jailbreaking.”<sup>13</sup> At present, it is unclear whether such an exemption is necessary because the case law is not settled. Courts have only applied § 1201 to TPMs that restrict usage of hardware platforms in a limited number of instances.<sup>14</sup> The two primary cases that address the topic do so in the context of garage door openers and printer toner cartridges, which may have narrow applicability to the Smartphone context.

This Note will apply the limited case law on § 1201 to a particular Smartphone lock-in, the Apple iPhone’s App Store lock-in, and conclude that iPhone jailbreaking is illegal without a specific exemption from the Library of Congress. The case law provides for both a formal approach and a functional approach to analyzing § 1201 liability. The Note argues that under the formal approach, jailbreaking liability turns on arbitrary idiosyncrasies of software design and circumvention method, obscuring the central intent behind the DMCA’s drafting—the protection of copyrighted works in the digital age. These idiosyncrasies are formed mostly at the discretion of software manufacturers, who can shape their products or tools in ways that may extend § 1201 protections to unintended applications, leaving § 1201 vulnerable to a myriad of anti-competitive practices and abuses. This Note proposes a functionalist approach to remedying the problem that would narrow the application of § 1201 through judicial interpretation in a manner consistent with the DMCA and the intent of its drafters.

Part I will introduce the topic by exploring the rationale behind iPhone modification. Part II will explicate the technical aspects of iPhone jailbreaking. Part III will assess jailbreaking liability under § 1201, focusing on the question of whether the iPhone Software “effectively controls access” to a copyrighted work. In particular, the Note will analyze iPhone Jailbreaking liability under the formalist framework set out in *Lexmark International, Inc. v. Static Control Components, Inc.*<sup>15</sup> and *Chamberlain Group, Inc. v. Skylink*

---

12. *Id.* at § 1201(a)(1)(D).

13. Comment of the Electronic Frontier Foundation, In re Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. RM 2008-8, Dec. 2, 2008, available at [http://www.eff.org/files/filenode/dmca\\_2009/EFF%2BRM%2Bproposals.pdf](http://www.eff.org/files/filenode/dmca_2009/EFF%2BRM%2Bproposals.pdf).

14. *See, e.g.*, *Lexmark Int’l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522 (6th Cir. Ky. 2004); *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 292 F. Supp. 2d 1023 (N.D. Ill. 2003).

15. 387 F.3d 522.

*Technologies, Inc.*<sup>16</sup> Part IV will discuss the problems associated with anti-circumvention abuse and propose a two-step analysis for courts to use when analyzing § 1201 liability in cases involving aftermarket goods or services.

## II. THE RATIONALE BEHIND IPHONE MODIFICATION

The iPhone locks its users into many different services, but two lock-ins have been and continue to be of particular controversy: AT&T as the iPhone user's exclusive wireless provider, and the Apple App Store as the iPhone user's exclusive source of software applications. Apple maintains these lock-ins by building protective measures into the software operating system (iPhone Software) installed on every new iPhone.

Soon after the iPhone's initial release, users who were not content with Apple's lock-in regimes discovered methods to enable the phone's usage with other wireless providers (unlocking), and the installation of unauthorized programs (jailbreaking).<sup>17</sup> The iPhone Software must be modified in both processes. Although exact figures are unknown, varying estimates have placed the number of jailbroken phones at somewhere between ten to twenty-five percent of all iPhones in operation.<sup>18</sup>

Apple's iPhone Software is the focal point of any jailbreaking analysis. The iPhone Software has protection under copyright law and the DMCA. However, unlike recent debates surrounding digital copyright and content piracy, iPhone jailbreaking centers not on the copyrighted work but on the restrictions placed on a hardware device through a copyrighted software operating system. In the case of the iPhone, many functions such as weather reports and stock quotes are only available through sources designated by Apple.<sup>19</sup> By purchasing an iPhone, a user automatically enters into several

---

16. 292 F. Supp. 2d 1023.

17. Jenna Wortham, *Unofficial Software Incurs Apple's Wrath*, N.Y. TIMES, May 13, 2009, at B1.

18. Scott Hillis, *Quarter of Apple iPhones may be unlocked: analyst*, REUTERS, Jan. 28, 2008, <http://www.reuters.com/article/idUSN2832924620080129>; Brian X. Chen, *Rejected By Apple, iPhone Developers Go Underground*, WIRED, Aug. 6, 2009, <http://www.wired.com/gadgetlab/2009/08/cydia-app-store>.

19. Physical addresses are "hotlinked" to Google Maps; Weather and Finance Apps are tied to Yahoo. Music and ringtones must be downloaded from, or loaded into, iTunes or the App Store. See Apple, Inc., *Activating Your original iPhone in the United States*, <http://support.apple.com/kb/HT1381> (last visited Jan. 29, 2010); Apple, Inc., *iPhone User Guide* at 71–85, 107–124, [http://manuals.info.apple.com/en\\_US/iPhone\\_User\\_Guide.pdf](http://manuals.info.apple.com/en_US/iPhone_User_Guide.pdf), at 10 (last visited Jan. 29, 2010).

lock-in arrangements, most notably with AT&T Wireless and the Apple App Store.<sup>20</sup>

These lock-ins are consummated by the user's acceptance of Apple's end-user license agreement (EULA) shortly after purchase. In the normal course of use, most iPhone purchasers will accept Apple's EULA at least two times. The user first agrees to the shrinkwrap contract on the iPhone's physical packaging and then again in the form of a clickwrap contract during the initial synchronization event between the iPhone and Apple's iTunes software.<sup>21</sup> The iPhone EULA dictates that a user "may not copy, decompile, reverse engineer, disassemble, attempt to derive the source code of, modify, or create derivative works of the iPhone Software," and that Apple "retain[s] ownership of the iPhone Software itself."<sup>22</sup> A user must click "Agree" in order to finish the setup. The acceptance of these terms provides a contractual basis on which Apple reinforces its lock-ins. However, even explicit notice is not effective for people who do not read it or fully integrate it into their decisions (before and at the point of sale).<sup>23</sup> As a result, despite their acquiescence to Apple's contractual terms, some users will still look to unlocking and jailbreaking to avoid being subject to iPhone lock-ins.

#### A. UNLOCKING: THE AT&T LOCK-IN

In most circumstances, the purchase and use of an Apple iPhone requires signing a two-year wireless service contract with AT&T.<sup>24</sup> Vendor lock-ins of this type are not unusual in the U.S. mobile phone market. Wireless carriers subsidize the price of handsets in exchange for committing to a term of service.<sup>25</sup>

Unlocking provides users with significant benefits. For instance, it allows users to purchase local phone plans while abroad, saving money. Also, if

---

20. See Apple, Inc., iPhone End-User License Agreement, [http://store.apple.com/Catalog/US/Images/iphone\\_tcs.pdf](http://store.apple.com/Catalog/US/Images/iphone_tcs.pdf) (last visited Jan. 29, 2010).

21. See *id.*

22. iPhone End-User License Agreement, *supra* note 20, at §§ 1, 3(c).

23. Molly S. Van Houweling, *The New Servitudes*, 96 GEO. L.J. 885, 933 (2008).

24. Apple, Inc., Buy iPhone 3G, <http://www.apple.com/iphone/buy> (last visited Jan. 29 2010) (disclaiming that discounted pricing is contingent upon a two year service contract). Users can purchase iPhones without a contract if they are willing to pay four hundred dollars more for an unsubsidized iPhone. Although this option is not widely publicized, it is probably safe to assume that since full priced iPhones are locked-in to the AT&T network, most normal customers will opt for the discounted pricing with the service contract. Prior to the release of the iPhone 3G, consumers could purchase the handset at the discounted price without signing a service contract with AT&T. See *AT&T to sell iPhone without contract for \$599*, ASSOCIATED PRESS, Mar. 19, 2009, available at <http://www.msnbc.msn.com/id/29779285/>.

25. Frieden, *supra* note 4, at 4.

users' needs become incompatible with a carrier's wireless coverage, unlocking allows the user to switch to another carrier without buying a new handset.<sup>26</sup> In recent years, the industry has sanctioned the practice of unlocking or removing the restrictions that bind a handset to a specific carrier for a certain amount of time.<sup>27</sup> However, AT&T refuses to unlock iPhones at any point in time, even after the contract expires, a potentially serious and costly inconvenience to many users.<sup>28</sup>

#### B. JAILBREAKING: APPLE APP STORE LOCK-IN

The iPhone is preloaded with software preventing the installation of new programs except those expressly authorized by Apple through its App Store. Critics such as the Electronic Frontier Foundation (EFF) claim that Apple, by technologically excluding competitors, forces both developers and consumers of iPhone applications to use the App Store.<sup>29</sup> iPhone App Store developers must submit all new applications or programs to Apple for approval. If an application is approved, only then can it be downloaded and installed through the App Store.<sup>30</sup>

As the gatekeeper to new programs and functionalities on the iPhone, Apple possesses a powerful mechanism to reinforce its App Store lock-in. As a matter of policy, the Apple App Store denies submissions or removes accepted applications that duplicate existing or planned iPhone capabilities.<sup>31</sup> For example, in June of 2009, Apple drew significant criticism over its reported rejection of the Google Voice application, prompting an investigation by the Federal Communications Commission.<sup>32</sup> Apple later

---

26. John Haubenreich, Note, *The iPhone and the DMCA: Locking the Hands of Consumers*, 61 VAND. L. REV. 1507, 1508 (2008). See generally SIM Lock, [http://en.wikipedia.org/wiki/SIM\\_lock](http://en.wikipedia.org/wiki/SIM_lock) (last visited Jan. 29 2010).

27. See Rob Pegoraro, *It's Not The Money, Can You Hear Me?*, THE WASHINGTON POST, May. 29, 2008, <http://www.washingtonpost.com/wp-dyn/content/article/2008/05/28/AR2008052803089.html>. Users can either unlock their phones after 90 days of service or at the end of one or two year contract with AT&T, T-Mobile, and Nextel, among others.

28. Leslie Cauley, *Handcuffs chafe wireless users*, USA TODAY, Aug. 22, 2007, [http://www.usatoday.com/tech/wireless/2007-08-22-cellphones-abroad\\_N.htm?csp=34](http://www.usatoday.com/tech/wireless/2007-08-22-cellphones-abroad_N.htm?csp=34).

29. Comment of the Electronic Frontier Foundation, *supra* note 13.

30. Posting of Paul Miller to Engadget, <http://www.engadget.com/2008/03/06/apple-announces-app-store-for-iphone-ipod-touch/> (Mar. 6, 2008, 00:48 PST).

31. See Chris Foresman, *Schiller's spin on App Store issues ignores real complaints*, ARS TECHNICA, Nov. 23, 2009, <http://arstechnica.com/apple/news/2009/11/schillers-spin-on-app-store-issues-ignores-actual-complaints.ars>; Posting of Josh Pigford to The Apple Blog, <http://theappleblog.com/2008/09/13/why-apples-app-store-approval-process-is-broken/> (Sep. 13, 2008, 01:18 MST); Daring Fireball, [http://daringfireball.net/2008/09/app\\_store\\_exclusion](http://daringfireball.net/2008/09/app_store_exclusion) (Sep. 12, 2008).

32. Erica Ogg, *Apple sheds light on App Store approval process*, CNET, Aug. 21, 2009, [http://news.cnet.com/8301-13579\\_3-10315328-37.html](http://news.cnet.com/8301-13579_3-10315328-37.html).

claimed that the app had not been rejected and was still under study, but stated that the application appears “to alter the iPhone’s distinctive user experience by replacing the iPhone’s core mobile telephone functionality and Apple user interface with its own user interface for telephone calls, text messaging and voicemail.”<sup>33</sup> Additional reports of stalled and indefinitely delayed applications have also prompted accusations of anticompetitive behavior.<sup>34</sup> Some iPhone application developers have complained about delayed payouts, inconsistent or stringent decency requirements, and arbitrary submissions denials.<sup>35</sup> While Apple has worked to increase the transparency of its approval system, many developers are still very unhappy with the process.<sup>36</sup> Facing rejection, some developers turn to publishing their applications on unofficial app stores that require jailbroken phones.<sup>37</sup>

Underpinning the grievances of some end-users and developers is the expectation of rights associated with traditional property ownership, whereby owners of a product (particularly related to hardware) are entitled to change and modify it as they see fit. Operating under this assumption, some iPhone users have turned to jailbreaking and unlocking to remedy what they perceive as an unreasonably restrictive set of lock-in regimes.

---

33. Apple.com, Apple Answers FCC’s Questions, <http://www.apple.com/hotnews/apple-answers-fcc-questions/> (last visited Jan. 29, 2010).

34. The App Store’s Exclusionary Policies, *supra* note 31.

35. See, e.g., Bill Ray, *Apple Joins Campaign for Real Breasts*, THE REGISTER, Jan. 16, 2009, [http://www.theregister.co.uk/2009/01/16/apple\\_boobs\\_again/](http://www.theregister.co.uk/2009/01/16/apple_boobs_again/) (reporting the acceptance of an application that allows users to animate nude body parts, while a cartoon version with similar functionality was rejected); Tom Krazit, *Apple nixes ‘potentially offensive’ South Park app*, CNET, Feb. 17, 2009, [http://news.cnet.com/8301-13579\\_3-10165736-37.html](http://news.cnet.com/8301-13579_3-10165736-37.html) (reporting the rejection of an application based on a cartoon for profanity, while the uncensored movie version of the cartoon was sold in the iTunes Store); Rik Myslewski, *Apple snips Nine Inch Nails app*, THE REGISTER, May 9, 2009, [http://www.theregister.co.uk/2009/05/04/nine\\_inch\\_nails\\_censorship/](http://www.theregister.co.uk/2009/05/04/nine_inch_nails_censorship/) (discussing the rejection of an application that plays songs from a well-known band due to the use of one profane word in its lyrics); see also Posting of Jim Dalrymple to Macworld, [http://www.macworld.com/article/134698/2008/07/app\\_store\\_developers.html](http://www.macworld.com/article/134698/2008/07/app_store_developers.html) (Jul. 25, 2008 00:00 PST).

36. Christian Zibreg, *Apple launches App Store Resource Center to ease submissions*, GEEK.COM, Sep. 21, 2009, <http://www.geek.com/articles/mobile/apple-launches-app-store-resource-center-to-ease-submissions-20090921/>.

37. Christian Zibreg, *iPhone: Renegade app store opens but Apple wants to kill it*, TG DAILY, Mar. 9, 2009, <http://www.tgdaily.com/software-features/41662-iphone-renegade-app-store-opens-but-apple-wants-to-kill-it/>.

### III. A TECHNICAL INTRODUCTION TO JAILBREAKING

The first jailbreaking method was introduced in July of 2007, approximately one month after the iPhone's initial release date.<sup>38</sup> Since then, a handful of internet communities have coalesced around the goal of defeating the iPhone's lock-in protections.<sup>39</sup> As the popularity of the iPhone grew, a technical "arms race" emerged between Apple and the iPhone jailbreaking/unlocking community, resulting in an "elaborate game of whack-a-mole as rogue programmers quickly counter[ed Apple's] efforts with their own software updates."<sup>40</sup>

During the iPhone's first three years on the market, Apple released more than twenty versions of the iPhone Software.<sup>41</sup> Many of these were jailbroken by tools widely available on the Internet.<sup>42</sup> In addition to providing new features and bug fixes, new iterations of the iPhone Software closed security loopholes exploited by iPhone jailbreakers and unlockers.<sup>43</sup> As a result, the process of jailbreaking an iPhone varies depending on the version of iPhone Software in operation.<sup>44</sup>

When the iPhone is first turned on, the iPhone Software executes a series of authenticity checks called the "chain of trust" before loading the operating system and other iPhone components.<sup>45</sup> This initial set of authenticity checks uses encryption keys to ensure that all iPhone firmware components are

---

38. Posting of Thomas Ricker to Engadget, <http://www.engadget.com/2007/07/10/iphone-hackers-we-have-owned-the-filesystem/> (Jul. 10, 2007, 07:05 PST).

39. For more background on the iPhone Jailbreaking community, see Brian X. Chen, *Jailbreakers Battle Apple for Control of iPhone*, WIRED, <http://www.wired.com/gadgetlab/2009/11/jailbreak-community/>.

40. Wortham, *supra* at note 17. While most of the focus (particularly in the press) has been centered on breaking the AT&T-Apple and Apple App Store lock-ins, unlocking or adding new features to the iPhone has been an equally important motivator of iPhone modification. Features are often unlocked or added through jailbreaking, followed quickly by an iPhone Software update from Apple that incorporates some features lacking in the previous iPhone Software release. The first jailbreaking method was initially designed to allow the installation of custom wallpapers and ringtones, a function that was later unlocked in version 1.1.3. An App Store for jailbroken phones had started to be used starting in version 1.1.2. Six months later, the Apple App Store was released as part of version 2.0. This process continues to this day. *See id.*

41. iPhone OS Version History, [http://en.wikipedia.org/wiki/IPhone\\_OS\\_version\\_history](http://en.wikipedia.org/wiki/IPhone_OS_version_history) (last visited Jan. 20, 2010).

42. *See infra* note 45.

43. *Id.*

44. *Id.*

45. Maria Colenso, *Jailbreaking your iPhone*, HOWSTUFFWORKS.COM, Apr. 14, 2009, <http://electronics.howstuffworks.com/how-to-tech/how-to-jailbreak-iphone1.htm/>. A chain of trust involves the validation of key hardware and software components in a device. It is intended to ensure that only trusted software and hardware is being used.

legitimate and unadulterated.<sup>46</sup> Despite differences in method, all jailbreaking solutions aim to disable this initial set of authenticity checks by exploiting a vulnerability that allows the jailbreaker to load a custom set of computer code, or payload, onto the iPhone.<sup>47</sup>

In its default state, the iPhone Software only allows the user to access the file system's "/private/var/mobile/Media" directory.<sup>48</sup> Jailbreaking allows the user to break out of this "jail" and reset access to "/" or top-level access to the entire file system (also known as privilege escalation), allowing for the custom payload to be copied onto the iPhone.<sup>49</sup> Once copied and then executed, the custom payload can exploit the iPhone's other vulnerabilities, allowing a jailbreaker to disable or modify the iPhone's chain of trust.<sup>50</sup> The payload disables several components in the iPhone operating system that prevent the execution of programs lacking Apple's encrypted digital signature.<sup>51</sup> Without jailbreaking, unsigned applications cannot be loaded onto the iPhone, and even if loaded, would not run.

iPhone jailbreaks generally fall into two categories depending on where the act of circumvention takes place. The most prevalent method of jailbreaking currently in use, "firmware restore," circumvents the iPhone Software's protective measures on the user's personal computer.<sup>52</sup> It involves downloading Apple's authorized iPhone Software onto a computer, then decrypting, unpacking, modifying, and repackaging it into a new file.<sup>53</sup> This is generally done using a software package custom-written by a party who also reverse-engineers and supplies the necessary cryptographic keys.<sup>54</sup> The modified iPhone Software is then "restored" onto the iPhone using iTunes

---

46. *See id.*

47. *See, e.g.*, Jailbreak, <http://theiphonewiki.com/wiki/index.php?title=Jailbreak> (last visited Jan. 29, 2010); How to Unlock/Jailbreak Your 2.0 2G iPhone (Windows), <http://www.iclarified.com/entry/index.php?enid=1572> (last visited Jan. 29, 2010).

48. iPhone Forensic Examinations – A Series #2, <http://mobileforensics.wordpress.com/2008/09/17/iphone-forensics-a-series-2/> (Sep. 17, 2008, 7:20 PST); *see also* /private/var, The iPhone Wiki, <http://theiphonewiki.com/wiki/index.php?title=/private/var> (last visited Jan. 29, 2010). Subdirectories of "/private/var/mobile/Media" are also accessible.

49. iPhone Forensic Examinations – A Series, <http://mobileforensics.wordpress.com/2008/09/17/iphone-forensics-a-series/> (Sep. 15, 2008, 7:16 PST).

50. *Id.*

51. *Id.*

52. For a complete discussion of firmware restore, see JONATHAN ZDZIARSKI, IPHONE FORENSICS 30–41, (O'Reilly Media 2008); TheiPhonewiki.com, Pwnage, <http://theiphonewiki.com/wiki/index.php?title=Pwnage> (last visited Jan. 29, 2010).

53. *Id.* This process involves making an unauthorized copy of the iPhone Software.

54. *Id.* TheiPhonewiki.com Mounting Ramdisk, [http://theiphonewiki.com/wiki/index.php?title=Mounting\\_ramdisk\\_of\\_ipsw\\_beta\\_4-7](http://theiphonewiki.com/wiki/index.php?title=Mounting_ramdisk_of_ipsw_beta_4-7) (last visited Jan. 29, 2010).

through a process originally designed to return the device to its factory default settings.<sup>55</sup>

Another type of jailbreaking involves circumvention of protective measures on the iPhone itself. These methods are still in use today but were more widely used during the first year of the iPhone's initial release. Two of the most popular methods exploited flaws in the iPhone's Universal Serial Bus (USB) connection and the iPhone Software's Safari browser.<sup>56</sup> These jailbreaks involved exploiting loopholes to enable some form of unrestricted communication with the iPhone. Once established, the iPhone Software's security measures are compromised externally (with the help of a custom designed website or a special jailbreaking program on the user's personal computer). Jailbreaking that takes place on the iPhone itself can be analogized to an attack that tunnels underneath a castle's walls, while firmware restore is equivalent to the planting of a Trojan horse. It is also

---

55. See ZDZIARSKI, *supra* note 51; Pwnage, *supra* note 52.

56. These are also known as the Apple File Connection (AFC) and Library Tiff (LibTiff) Jailbreaks. AFC is a program that facilitates limited access to the iPhone file system for interoperability with desktop computers. The AFC program allows the iPhone to share photos, music, and address book contacts over a USB connection by permitting open access to the iPhone's "/private/var/mobile/Media" directory, but prohibiting access to the rest of the file system. Jailbreakers exploited vulnerabilities in the iPhone's AFC to modify a critical chain of trust component called iBoot. When the iPhone was restarted, iBoot then granted privilege escalation, allowing for access to the entire file system and the loading of custom payload that disables the operating system's digital signature verification components. *Id.*; see iPhone Hacking, First Steps, <http://www.wrightthisway.com/Articles/000428.html> (Aug. 16, 2007, 21:53 PST).

Probably the most infamous of these jailbreaks involved taking advantage of the LibTiff vulnerability in version 1.1.1 of the iPhone firmware. LibTiff is a software component that enables the viewing of a certain Tag Image File Format (Tiff) image files. In iPhone versions 1.1.1 and earlier, LibTiff was prone to buffer-underflow and overflow vulnerabilities that involved the program receiving data at a faster or slower rate than was acceptable. This problem is typically prevented by built-in "boundary checks" that regulate the flow of data, but the iPhone's LibTiff component was not programmed to conduct enough of these checks. Although in most cases this flaw would result in crashed applications and other system errors, this vulnerability could be exploited in a way where a maliciously crafted Tiff image file could be used to execute unauthorized programs on the iPhone. Although several different jailbreaking solutions were developed based on this flaw, the most popular method involved visiting the Jailbreakme.com website using the iPhone's Safari web browser. The site contained a custom Tiff image that exploited the flaw and uploaded a custom payload onto the iPhone's file system, which then jailbroke the iPhone and patched LibTiff vulnerability, creating an arguably more secure device. Ryan Block, *iPhone and iPod touch v1.1.1 full jailbreak tested, confirmed!*, ENGADGET, available at <http://www.engadget.com/2007/10/10/iphone-and-ipod-touch-v1-1-1-full-jailbreak-tested-confirmed/>. See also Juniper Networks, *LibTIFF 'tif\_lzw.c' Remote Buffer Underflow Vulnerability*, <http://www.juniper.net/security/auto/vulnerabilities/vuln30832.html> (last visited Apr. 17, 2010).

important to note that firmware restore has been the dominant method of jailbreaking since the release of firmware 2.0 in mid 2008.<sup>57</sup>

#### IV. LIABILITY FOR JAILBREAKING UNDER SECTION 1201 OF THE DMCA

The act of jailbreaking an iPhone may create liability in three ways: breach of contract, copyright infringement, and as an act of illegal circumvention. Apple is unlikely to pursue breach of contract claims against its users for acts of personal use due to the difficulty of proving a significant amount of actual damages and the public relations fallout likely to result from suing its own customers. Apple is in a better position to protect iPhone technology by enforcing its software copyrights. 17 U.S.C. § 106 provides copyright owners with exclusive rights to authorize reproduction, creation of derivative works, and distribution.<sup>58</sup> Apple has claimed that depending on the method used, jailbreaking violates at least one of these exclusive rights.<sup>59</sup> Although jailbreaking could qualify as copyright infringement of Apple's two federally registered copyrights for the iPhone software,<sup>60</sup> this Note will discuss these issues only to the extent that they impact liability for illegal circumvention.

In 1998 Congress enacted § 1201 as part of Title I of the DMCA to address the growing piracy concerns of content owners and promote the electronic availability of digital works on the Internet.<sup>61</sup> The DMCA punishes

---

57. See Jailbreak, *supra* note 47.

58. 17 U.S.C. § 106(1)(3) (2006).

59. Response of Apple, *supra* note 10 at 2.

60. See Copyright Registration No. TX0006457868 (registered Sept. 13, 2007), available at <http://cocatalog.loc.gov>; Copyright Registration No. TX0006871140 (registered Oct. 10, 2008), available at <http://cocatalog.loc.gov>.

61. Section 1201 of the DMCA was initially introduced as the "WIPO Copyright Treaties Implementation Act." It brought U.S. law in compliance with the WIPO Performances and Phonograms Treaty entered into by the Clinton Administration during the Geneva conference. See H.R. REP. NO. 105-551, pt. 1 (1998). Congress posited that the dissemination of copyrighted works on the Internet is contingent upon the adequate digital protection for copyright owners. *Id.* Likening HR 2815 to the prohibitions on the circumvention of satellite and cable television technologies, Congress saw the need to secure these digital protections. *Id.* Recognizing that the Internet and the digitization of copyrighted works represent a unique threat to the rights of copyright owners, the Commerce committee concluded that:

the digital environment poses a unique threat to the rights of copyright owners, and as such, necessitates protection against devices that undermine copyright interests. In contrast to the analog experience, digital technology enables pirates to reproduce and distribute perfect copies of

those who would “try to profit from the works of others by decoding the encrypted codes protecting copyrighted works, or engaging in the business of providing devices or services to enable others to do so.”<sup>62</sup>

Unlike most cases involving the DMCA, where unauthorized access is being used to copy unauthorized copyrighted content,<sup>63</sup> the act of jailbreaking an iPhone does not circumvent access to copyrighted content offered on Apple’s iTunes or App Store. Apple provides three types of copyrighted works through its content delivery platforms: video, audio, and applications. These works are subject to varying degrees of access control mechanisms in the form of Digital Rights Management (DRM) schemes.<sup>64</sup> The process of jailbreaking involves the execution of custom software designed to disable authenticity checks on critical iPhone software components, without modifying any of Apple’s built-in DRM encryption systems for its copyrighted works.<sup>65</sup>

However, jailbreaking does indirectly modify access control mechanisms that safeguard copyrighted content. Jailbreaking enables user access to the iPhone’s file system, which is disabled by default.<sup>66</sup> Although not specifically altering a DRM protection, jailbreaking does make it easier for users to access DRM-protected files on the Apple iPhone. The usefulness of this feature is somewhat limited, as users are readily able to access the same

works-at virtually no cost at all to the pirate. As technology advances, so must our laws.

Report of the U.S. House Comm. on Commerce, H.R. REP. NO. 105-551, pt. 2, at 25 (1998). Pamela Samuelson, however, has criticized this view and claims that “the DMCA went far beyond treaty requirements in broadly outlawing acts of circumvention of access controls and technologies that have circumvention-enabling uses.” Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need To Be Revised*, 14 BERKELEY TECH. L.J. 519, 521 (1999). Professor Samuelson goes on to state that “Hollywood and its allies sought the strongest possible ban both on the act of circumventing a technical protection system used by copyright owners to protect their works and on technologies having circumvention-enabling uses.” *Id.* at 522–23.

62. H.R. REP. NO. 105-551.

63. *See, e.g.*, *Universal City Studios v. Corley*, 273 F.3d 429 (2d Cir. 2001) (finding copyright controls on DVDs to be eligible for § 1201 protection); *RealNetworks, Inc. v. Streambox, Inc.*, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. 2000) (capturing streaming video).

64. Audio works are essentially free of DRM protections as of early 2009. All applications and almost all video works distributed by Apple are protected by the Fairplay DRM scheme. *iTunes Store and DRM-free music: What you need to know*, MACWORLD, [http://www.macworld.com/article/138000/2009/01/drm\\_faq.html](http://www.macworld.com/article/138000/2009/01/drm_faq.html) (last visited Jan. 29, 2010).

65. TheiPhonewiki.com, Copy Protection Overview, [http://www.theiphone.wiki.com/wiki/index.php?title=Copy\\_Protection\\_Overview](http://www.theiphone.wiki.com/wiki/index.php?title=Copy_Protection_Overview) (last visited Jan. 29, 2010).

66. *See* Zdziarski, *supra* note 52.

DRM-protected content on their home computer in iTunes without any file system protections. Nevertheless, there is some credence to the claim that jailbreaking detracts from iPhone security and the integrity of Apple's DRM architecture.<sup>67</sup> Third-party applications designed to work with jailbroken iPhones have broken Apple's Fairplay copy protections and pirated versions of App Store games and applications are widely available on the Internet.<sup>68</sup>

A. SECTION 1201 OF THE DMCA

Section 1201(a)(1) of the DMCA provides that no persons shall circumvent "a technological measure that effectively controls access to a [copyrighted work]."<sup>69</sup> The House of Representatives likened violations of § 1201(a)(1) to the act of breaking into a locked room to obtain a copy of a book, rather than the use of the book itself.<sup>70</sup>

Section 1201(a)(2), the anti-trafficking prohibition, outlaws trafficking in certain products and services that "aid and abet" those circumventing access control measures referred to in § 1201(a)(1).<sup>71</sup> Both §§ 1201(a)(1) and 1201(a)(2) seek to prevent circumvention, as § 1201(a)(1) prohibits the act itself and § 1201(a)(2) punishes accomplices.

Also, § 1201(b)(1) prohibits trafficking in devices that circumvent rights protection measures ("rights circumvention trafficking").<sup>72</sup> As two closely related yet distinct prohibitions, § 1201(a)(2) penalizes trafficking in devices that circumvent measures safeguarding initial access, while (b)(1) implicates those who provide the tools that circumvent measures that secure the

---

67. FairPlay is Apple's proprietary digital rights management system; it secures all content sold through the Apple iTunes and App Stores. Apple has argued that jailbreaking removes file system protections on the iPhone, thus easing access to Fairplay DRM schemes on the iPhone. *See* Response of Apple, *supra* note 9 at 14. This access, however, is widely available on personal computers where the file system is not locked, so the practical utility of an unlocked file system for breaking DRM schemes is questionable. Nevertheless, jailbreaking does remove a layer of protection on the iPhone and jailbroken apps that break Apple's Fairplay DRM have appeared. *See, e.g.*, Charlie Sorrel, Crackulous Strips Copy Protection from iPhone Apps, WIRED, <http://www.wired.com/gadgetlab/2009/02/crackulous-stri/>. *See also* How FairPlay Works: Apple's iTunes DRM Dilemma, <http://www.roughlydrafted.com/RD/RDM.Tech.Q1.07/2A351C60-A4E5-4764-A083-FF8610E66A46.html> (last visited Jan. 29, 2010).

68. *See id.* *See, e.g.*, IsoHunt.com, <http://isohunt.com/torrents/?ihq=iphone+apps> (a listing of pirated iPhone apps for download using the BitTorrent protocol) (last visited Jan. 29, 2010).

69. 17 U.S.C. § 1201(a)(1) (2006).

70. H.R. REP. NO. 105-551, pt. 1, at 35 (1998).

71. 17 U.S.C. § 1201(a)(2) (2006).

72. *Id.* at § 1201(b)(1).

copyright protections during lawful usage.<sup>73</sup> Copy controls, for example, would be a basis for § 1201(b)(1) liability but not under § 1201(a)(2), while initial access controls would be a basis for the reverse.<sup>74</sup> Unlike § 1201(a)(2), there is no violation for conduct in § 1201(b)(1):

Prior to [enactment of the DMCA], the conduct of circumvention was never before made unlawful. The device limitation in [§ 1201(a)(2)] enforces this new prohibition on conduct. The copyright law has long forbidden copyright infringements, so no new prohibition was necessary. The device limitation in [§ 1201(b)(1)] enforces the longstanding prohibitions on infringements.<sup>75</sup>

The statute defines circumvention as an act “to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner.”<sup>76</sup> As described, *supra*,<sup>77</sup> the process of jailbreaking involves numerous acts of bypassing, removing, and deactivating the iPhone Software restrictions meeting the statute’s definition of circumvention.<sup>78</sup> The iPhone Software itself is also very likely a “technological measure,” which according to Congress could be “based on encryption, scrambling, authentication, or some other measure which requires the use of a ‘key’ provided by a copyright owner to gain access to a work.”<sup>79</sup> The iPhone’s chain of trust, authenticity checks, digital signature checks, and restricted file system access are all examples of the iPhone’s technological measures, an interpretation supported by case law.<sup>80</sup>

Jailbreaking will always involve many separate acts of decryption aimed directly at circumventing the technical measures in a manner that is directly prohibited by the statute.<sup>81</sup> While the act of jailbreaking is likely to fall within the scope of “circumvention” under § 1201(a), in establishing a cause of action, a plaintiff must also prove that the circumvention is directed at a technical measure that “effectively controls access” to a copyrighted work.

---

73. *See id.*; *see also* Melville B. Nimmer & David Nimmer, 3 NIMMER ON COPYRIGHT § 12A.03 (2003).

74. *See id.*

75. S. REP. NO. 105-190, at 12 (1998).

76. 17 U.S.C. § 1201(a)(3)(A) (2006).

77. *See supra* Part II.

78. *Id.*

79. H.R. REP. NO. 105-796, at 43 (1998).

80. *See* Lexmark Int’l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 546 (6th Cir. 2004) (finding an encrypted authentication process to be a technological measure).

81. *See supra* Part II.

Congress did not expressly address whether § 1201 applied to the circumvention of software technological protection measures (TPMs) that control access not only to the software itself, but also to aftermarket hardware or services. In cases where the copyrighted work is a piece of software that is in itself the technical measure and the gatekeeper to some hardware functionality (like the iPhone), the question of whether the technical measure actually “effectively controls access” becomes an issue of judicial interpretation.

B. *LEXMARK INTERNATIONAL V. STATIC CONTROL*

1. *The “Effectively Controls Access” Standard for Section 1201 Liability*

In interpreting § 1201 to resolve a matter not anticipated by Congress, the Sixth Circuit Court of Appeals in *Lexmark Int’l, Inc. v. Static Control Components* employed a formalistic analysis of the statute’s “effectively controls access” language to carve out certain exemptions from § 1201 liability.<sup>82</sup>

In *Lexmark*, a toner cartridge manufacturer was enjoined from further distribution of a toner cartridge microchip that circumvented a copyrighted program that prevented the use of unauthorized toner cartridges with Lexmark printers.<sup>83</sup> The copyrighted work was Lexmark’s Printer Engine Program (PEP), which also controlled many of the printer’s essential functions.<sup>84</sup> The defendants created SMARTEK chips containing an exact copy of Lexmark’s PEP that allowed for unofficial toner cartridges to be used with Lexmark printers.<sup>85</sup> The PEP on SMARTEK chips permitted consumers to satisfy an authentication procedure that occurred each time the printer door was opened and closed.<sup>86</sup>

The district court found that: (1) Lexmark’s authentication sequence constituted a “technological measure that controls access” to two different copyrighted works within the printer itself, and (2) circumvention of these measures was within the scope of § 1201 liability.<sup>87</sup> The Sixth Circuit overturned this decision, holding that it was not Lexmark’s authentication sequence that “controls access” to the PEP, but rather the purchase of the printer itself—since anyone who owned a Lexmark Printer was free to read the code.<sup>88</sup> As a result, the Court of Appeals held that there was no effective

---

82. *Lexmark*, 387 F.3d 522.

83. *Id.* at 529, 532.

84. *Id.*

85. *Id.* at 530.

86. *Id.*

87. *Id.* at 532.

88. *Id.*

access control to the PEP code and therefore the defendant was not liable under § 1201.<sup>89</sup>

In its discussion of the computer code of the PEP, the Court of Appeals identified two different types of access: functional and literal.<sup>90</sup> Functional access refers to the use of what results from the execution of computer code, while literal access allows the user to view the code in its programming language format.<sup>91</sup> In *Lexmark*, the plaintiff's authentication sequence blocked functional access to the printer preventing its operation, but did not restrict access to the literal programming code of the PEP.<sup>92</sup>

Thus, the Court of Appeals held that because the authentication process controlled only functional access to the PEP, it did not fall within the purview of the DMCA because § 1201 does not cover authentication measures controlling access to “otherwise-readily-accessible copyrighted works.”<sup>93</sup> The court opined that a lock on the back door of a house cannot possibly be said to “control access” to that house if there is no lock on the front door.<sup>94</sup>

2. *Are the iPhone's Technological Protection Measures Protected under Lexmark?*

In *Lexmark*, the plaintiffs used § 1201 to secure a hardware device (the printer). The actual copyrighted software involved was of relatively minor concern, a drastic departure from the issue in traditional DMCA cases.<sup>95</sup> The key is to determine where iPhone jailbreaking fits along this spectrum, and if it falls within the *Lexmark* exemption. The first step in this determination is an analysis of the iPhone's TPMs under *Lexmark*.

Two relevant TPMs exist: the encryption protecting the iPhone Software (while on a user's personal computer) and the iPhone Software itself (after its installation on the iPhone).<sup>96</sup> In its packed and encrypted state on the hard drive of the user's computer, the iPhone Software lacks functionality and its encryption is a TPM that prevents the user from literal access to the iPhone's code.<sup>97</sup> On the iPhone device, the iPhone Software itself is a TPM which

---

89. *Id.* at 551.

90. *Id.* at 548.

91. *Id.*

92. *Id.* at 549.

93. *Id.*

94. *Id.* at 547.

95. *See, e.g.,* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001); RealNetworks, Inc. v. Streambox, Inc., 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. 2000).

96. *See supra* notes 45, 47, 52.

97. *Id.*

prohibits access to the literal code and restricts access to functional software components.<sup>98</sup>

Both iPhone TPMs are highly distinguishable from those that control access to the PEP in *Lexmark*. The PEP authentication process restricts functional access, and does so in a binary fashion that either grants or denies the user access to the basic functionality of the printer.<sup>99</sup> The TPMs in the iPhone Software similarly restricts access to the functionality of the iPhone, but in a far more nuanced and complicated manner. These TPMs restrict access to certain subsets of the iPhone Software.<sup>100</sup> For example, if the iPhone were to be used with a carrier other than AT&T, the device's phone application will not function.<sup>101</sup> The file system is also sealed off from user access and the installation of applications not authorized by Apple is not allowed.<sup>102</sup> iPhone TPMs also entirely prohibit literal access to the iPhone Software code, both on the user's computer and on the iPhone handset.<sup>103</sup>

Under *Lexmark*'s exemption of "otherwise readily available" works from § 1201 liability, iPhone TPMs likely qualify for DMCA protection. Unlike the TPMs in *Lexmark* that merely controlled access to an "otherwise readily available work," iPhone TPMs restrict both functional and literal access to the iPhone Software—always protecting the literal code of the iPhone Software and heavily restricting the functional elements of user access. Out of the box, the current model of the iPhone is essentially nonfunctional. Aside from an option that allows the user to make emergency calls, access to the functionality of the iPhone software is entirely prohibited. Apple or AT&T must "activate" the iPhone in-store to allow for basic functional access. Even after such access is granted, iPhone TPMs continue to restrict access to the iPhone software's functional components.

Moreover, the court in *Lexmark* held that because:

Lexmark has not directed any of its security efforts, through its authentication sequence or otherwise, to ensuring that its copyrighted work (the Printer Engine Program) cannot be read and copied, it cannot lay claim to having put in place a "technological measure that effectively controls access to a work protected under [the copyright statute]."<sup>104</sup>

---

98. *Id.*

99. *See Lexmark*, 387 F.3d at 529–30.

100. *See supra* Part II.

101. *Id.*

102. *Id.*

103. *Id.*

104. *Lexmark*, 387 F.3d at 549.

As discussed, the iPhone TPMs, unlike those used in the PEP, do in fact protect the iPhone Software.

The court in *Lexmark* also distinguished the PEP from copyrighted works that had previously been the subject of § 1201 cases, theorizing that copyright protection under the DMCA “operates on two planes: in the literal code governing the work and in the visual or audio manifestation generated by the code’s execution.”<sup>105</sup> For example, “the encoded data on CDs translates into music and on DVDs into motion pictures, while the program commands in software for video games or computers translate into some other visual and audio manifestation.”<sup>106</sup> In these cases, restricting “use” of the work means restricting consumers from viewing or accessing the copyrightable expression that is the output of the literal software elements. The court found the output of the PEP program to be “purely functional,” operating on only one “plane of expression,” and as a result, not subject to § 1201.<sup>107</sup> In the court’s opinion, a literal program that merely controlled paper feed, movement, and motor control was not a form of copyrightable expression. Moreover, it is because the PEP “is not a conduit to protectable expression” that *Lexmark* chose not to protect the literal elements of the code.<sup>108</sup> As *Lexmark*’s authentication sequence did not restrict access to this literal code, the DMCA did not protect it from circumvention.<sup>109</sup>

In contrast, the audio and video manifestations outputted by the iPhone Software constitute the “front-end” or user interface for an entire mobile phone operating system. They far exceed the “purely functional” output of the PEP and likely qualify for § 1201 protection.

### 3. *Jailbreaking Liability under Lexmark*

The act of iPhone jailbreaking is likely a violation under § 1201(a)(1) and in certain cases §§ 1201(a)(2) and 1201(b)(1) as well. As discussed, *supra*,<sup>110</sup> iPhone jailbreaks generally belong in two categories based on where the circumvention takes place.

Regardless of the method, all jailbreaking solutions aim to achieve three goals: (1) to disable the authenticity checks during the many transitional steps of booting the device, (2) to disable the digital signature checks present in the core of the operating system, permitting program code not signed by Apple

---

105. *Id.* at 548.

106. *Id.*

107. *Id.* at 547.

108. *Id.* at 549.

109. *Id.*

110. *See supra* notes 52–57 and accompanying text.

to run, and (3) to modify read/write permissions to gain access to the entire iPhone file system.<sup>111</sup>

Jailbreaking that takes place on the computer through firmware restore accomplishes all three goals by modifying the iPhone Software.<sup>112</sup> This method relies on decrypting and unpacking the software package downloaded from Apple.<sup>113</sup> The access control mechanism that firmware restore jailbreaking circumvents is the encryption that prevents access to the iPhone Software's literal code.<sup>114</sup> After modification, the user loads the modified iPhone Software onto the device granting unrestricted functional access.<sup>115</sup>

In contrast, modifying iPhone TPMs on the device itself involve one or more acts of decryption, exploitation and circumvention directed at hardware and software TPMs to accomplish each of the three goals of iPhone jailbreaking.<sup>116</sup> In this case, the TPMs being circumvented directly control the iPhone Software's functional access, and involve literal access only to the extent of breaking controls on iPhone operation.<sup>117</sup> Once the jailbreaking process has finished the custom payload grants literal access to the iPhone Software as part of the last step of the jailbreak.<sup>118</sup>

In comparing these two classes of jailbreaking methods, firmware restore is more likely to be prohibited under the DMCA as a direct circumvention of TPMs that control access to a copyrighted work. iPhone-based jailbreaks, on the other hand, occur after the user establishes essential functional access to the device and only grants access to the literal code to the extent necessary to free the iPhone from Apple's restrictions. This latter type of jailbreaking comes closer to the type of circumvention that bypasses access controls to "otherwise readily accessible works" and is therefore more likely to escape liability under the *Lexmark* rule.

Firmware restore is likely a violation of § 1201(a)(1) or 1201(a)(2) as either an act of illegal circumvention or illegal trafficking in circumvention technologies, respectively. These prohibitions punish acts that circumvent initial access. The iPhone Software in its unpacked and encrypted state, grants the user no access be it functional or literal.

---

111. *Id.*

112. *Id.*

113. *Id.*

114. *Id.*

115. *Id.*

116. *Id.*

117. *Id.*

118. *Id.*

On the other hand, iPhone-based jailbreaks do not always circumvent access control measures that safeguard initial access prohibited by §§ 1201(a)(1) and 1201(a)(2). These jailbreaks can be used either before or after the user has essential functional access, and may qualify as a basis for all three § 1201 violations depending on whether or not the device has basic functionality at the time of the jailbreak.

The dominant form of jailbreaking in use today, firmware restore, also happens to form the strongest basis for § 1201 liability. As a result, jailbreaking is very likely to be actionable under § 1201. Jailbreaking liability, in comparison to *Lexmark* where the court withheld § 1201 protections for the PEP, turns on a very mechanical distinction that may not be fully applicable to computer software.

#### 4. *Lexmark's Inapplicability to Computer Software Circumvention*

Under *Lexmark*, § 1201 liability is based on the formalist principle that one cannot break into something that is already accessible by other means. By holding that literal access cannot be protected when functional access is “otherwise readily available,” the *Lexmark* court has essentially equalized the treatment of literal and functional access in the context of computer software circumvention.

In the case of most computer software, functional and literal access has radically different implications. Literal access to the computer code grants inside knowledge of the structure and methodologies used to construct a computer program, but has no usefulness to the average user, and vice-versa for functional access. By holding that they are the same, the Court of Appeals in *Lexmark* essentially created a de facto exemption for circumvention of access controls that secure otherwise readily-accessible copyrighted works in the computer software context. All computer software is designed for the purposes of execution and operation. This operation will almost always have a functional component whereby the program actually accomplishes some task. Access to the functional component is typically not restricted to allow use of such a program by the consumer. *Lexmark* legitimizes the circumvention of access controls to the literal code whenever such software restrictions are absent. Applying *Lexmark* to iPhone jailbreaking, § 1201 liability appears to turn on a formalistic distinction that is more affected by software design than wrongfulness of conduct.

5. *The Interoperability Issue*

The DMCA exempts acts of circumvention necessary to achieve software interoperability.<sup>119</sup> The court in *Lexmark* addressed this issue and held that because the defendant copied Lexmark's works and did not use an independently created device in the act of circumvention, the defendant was not entitled to this defense.<sup>120</sup> Because the firmware restore method of jailbreaking does in fact copy and modify the iPhone software,<sup>121</sup> it would likely not fall under this exception.

C. *CHAMBERLAIN V. SKYLINK*

Another key case in interpreting the application of § 1201 to aftermarket hardware goods is *Chamberlain Group, Inc. v. Skylink Technologies*,<sup>122</sup> where a garage door opener (GDO) manufacturer brought a cause of action against the manufacturer of a universal remote for circumvention of wireless radio frequency code.<sup>123</sup> Skylink Technologies manufactured a universal GDO remote that replicated the functionality of a GDO remote made by the Chamberlain Group.<sup>124</sup> Skylink's universal GDO remote could "learn" the unique software code used to control Chamberlain GDOs and retransmit it.<sup>125</sup> Chamberlain filed suit under the § 1201(a)(2) of the DMCA, claiming that Skylink Technologies trafficked in universal remotes primarily designed "for the purpose of circumventing [Chamberlain's code] that effectively controls access to [their copyrighted computer programs]."<sup>126</sup> At trial, Chamberlain argued that Skylink violated § 1201(a)(2) for trafficking of circumvention technologies.<sup>127</sup> Skylink countered with the assertion that § 1201 can only be violated when the act of circumvention takes place without the authorization of the copyright owner.<sup>128</sup> Since it is Chamberlain's own customers who are committing the act of circumvention, Skylink posited that its manufacturing of universal GDO remotes is not actionable under § 1201(a)(2), because the underlying act of circumvention is not illegal. The district court agreed and held that Chamberlain did not explicitly restrict

---

119. 17 U.S.C. § 1201(f) (2006).

120. *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 525 (6th Cir. 2004).

121. *See supra* note 53.

122. 381 F.3d 1178 (Fed. Cir. 2004).

123. *Id.* at 1183–84.

124. *Id.*

125. *Id.*

126. *Id.* at 1187.

127. *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 292 F. Supp. 2d 1023, 1032 (N.D. Ill. 2003).

128. *Id.* at 1033.

the consumer's use of alternate GDO remotes and that this was deemed an unconditional sale that implicitly authorized customers to use other remotes.<sup>129</sup> The court also noted that Chamberlain's construction of the DMCA would force its own customers to violate § 1201.<sup>130</sup>

1. *Six-element Test for Jailbreaking under Chamberlain*

On appeal, the Federal Circuit set out a new six-element test that a plaintiff must prove to prevail in a § 1201(a)(2) trafficking action:

(1) ownership of a valid copyright on a work, (2) effectively controlled by a technological measure, which has been circumvented, (3) that third parties can now access (4) without authorization, in a manner that (5) infringes or facilitates infringing a right protected by the Copyright Act, because of a product that (6) the defendant either (i) designed or produced primarily for circumvention; (ii) made available despite only limited commercial significance other than circumvention; or (iii) marketed for use in circumvention of the controlling technological measure.<sup>131</sup>

The TPM in *Chamberlain*, much like that in *Lexmark*, secured access to a copyrighted work used primarily to control a mechanical device. In *Lexmark*, it was the basic functions of a printer, and in *Chamberlain* it was the opening of a garage door. Also similar to *Lexmark*, the *Chamberlain* TPM was itself a copyrighted work: the "rolling code" was both a TPM and a piece of copyrighted code for GDO communication.<sup>132</sup> The court found that a homeowner's access to this code had "no reasonable relationship" with Chamberlain's rights under the Copyright Act.<sup>133</sup> Key to this analysis was the court's interpretation of the legislative history behind § 1201. The court found that Congress did not intend for the DMCA to rescind the basic bargain of granting the public noninfringing and fair uses of copyrighted materials, and that therefore § 1201 "prohibits only forms of access that bear a reasonable relationship to the protections that the Copyright Act otherwise affords its owners."<sup>134</sup> As a result, the court held that for a circumvention to be prohibited by the DMCA, it must facilitate infringement of a right protected under the Copyright Act.<sup>135</sup>

---

129. *Id.*

130. *Id.*

131. *Id.* at 1203.

132. *Id.* at 1186.

133. *Id.* at 1204.

134. *Id.* at 1202.

135. *Id.* at 1204.

The court also found that the plaintiff's claim lacked the "critical nexus between access and protection," the fifth element in the court's § 1201(a)(2) framework,<sup>136</sup> and found no reasonable relationship "between the access that homeowners gain to Chamberlain's copyrighted software when using Skylink's Model 39 transmitter and the protections that the Copyright Act grants to Chamberlain."<sup>137</sup> The court also reasoned that the Copyright Act authorized Chamberlain's customers to use the copy of Chamberlain's software embedded in the GDOs that they purchased and were therefore immune from § 1201(a)(1) circumvention liability.<sup>138</sup> The court held that without a violation of § 1201(a)(1), there cannot be 1201(a)(2) liability.<sup>139</sup>

## 2. *Application of Chamberlain to the iPhone*

Under *Chamberlain's* central nexus test, we must first assess if the access gained from jailbreaking violates any of Apple's rights under the Copyright Act. 17 U.S.C. § 501 states that anyone who violates a copyright owner's exclusive rights is an infringer.<sup>140</sup> Jailbreaking the iPhone Software using the firmware restore method comprises of four potential infringements of Apple's exclusive right of reproduction per § 106(1).

The user first downloads the iPhone Software onto the user's computer as authorized by Apple's EULA.<sup>141</sup> Next, the user executes a custom-written jailbreaking application that copies the iPhone Software onto the computer's volatile RAM, the first unauthorized reproduction.<sup>142</sup> In *MAI Systems Corporation v. Peak Computer*, the unauthorized loading of copyrighted material from a hard disk into RAM for manipulation by a computer's central processing unit was found to be an infringement.<sup>143</sup>

The copy of the iPhone Software on the computer's RAM is then decrypted, unpacked, modified, and repacked.<sup>144</sup> The user is then prompted to specify a location on the computer's hard drive to save the modified file.<sup>145</sup> As the second act of infringement, the jailbreaking tool then copies the modified iPhone Software from the computer's RAM to its hard drive.<sup>146</sup> Next, the user launches Apple iTunes, which copies the modified iPhone

---

136. *Id.*

137. *Id.*

138. *Id.*

139. *Id.*

140. 17 U.S.C. § 501(a) (2006).

141. *See supra* note 20.

142. *Id.*

143. *MAI Sys. Corp. v. Peak Computer*, 991 F.2d 511, 518 (9th Cir. 1993).

144. *See supra* notes 52–55 and accompanying text.

145. *Id.*

146. *Id.*

Software to the computer's RAM and unpacks it and loads it onto the iPhone.<sup>147</sup> These are the third and fourth unauthorized copies. Given the unauthorized copying used in the firmware restore method, iPhone jailbreaking likely meets *Chamberlain's* "central nexus" test for liability due to the direct link between the act of circumvention and violations of the copyright owner's exclusive rights under 17 U.S.C. § 106.

Insofar as the issue of authorization, the iPhone Software is also distinguishable from *Chamberlain* in that Apple expressly prohibits jailbreaking through its clickwrap EULA,<sup>148</sup> and goes to retain ownership of the iPhone Software through a limited license, foreclosing any defense based on implied authorization. Under *Chamberlain*, jailbreaking is likely to be illegal under the DMCA.

*Chamberlain's* central nexus test does improve on the *Lexmark* approach for circumvention liability by linking § 1201 violations to essential rights of the copyright owner under § 106. It is, however, still subject to the constraints of a formalist distinction that turns on the technicality of whether a plaintiff can obtain rights under the Copyright Act. This formalistic analysis leaves § 1201 vulnerable to misuse by manufacturers who would employ copyright protections as a sword to reinforce their lock-in regimes, rather than a shield for the protection digital rights as envisioned by Congress.

#### D. LIBRARY OF CONGRESS EXEMPTION

Even under the current Library of Congress exemption for unlocking, jailbreaking's legality is highly suspect. In 2006, the Library of Congress created an exemption from § 1201 liability for "[c]omputer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network."<sup>149</sup> This is essentially a de facto exemption to § 1201 liability for unlocking mobile phones. Under the theory that jailbreaking is required for unlocking, the EFF and iPhone modification enthusiasts have claimed that jailbreaking is legal.<sup>150</sup>

However, the exemption does not expressly address the act of jailbreaking. More importantly, current unlocking methods are not designed for the "sole purpose" of wireless provider interoperability. In many iPhone

---

147. *Id.*

148. See iPhone End-User License Agreement, *supra* note 20.

149. Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works, 71 FED. REG. 64639 (Nov. 3, 2006).

150. Comment of the Electronic Frontier Foundation, *supra* note 29.

modification tools, unlocking is one of many features of a program designed chiefly for jailbreaking. In configuring how you jailbreak your phone, you can even chose not to unlock it. Some jailbreaking tools do not have unlocking features.<sup>151</sup> While it is technically possible for firmware restore to be used in a manner that strictly complies with the exemption, this is simply not the way the tools have been designed. Even assuming that unlocking necessitated jailbreaking, current unlocking solutions are not implemented in a way that fits within the language of the exemption.<sup>152</sup> As a result, the 2006 unlocking exemption likely does not cover jailbreaking, and until it gets its own exemption, jailbreaking is likely illegal under the DMCA.

## V. A FUNCTIONALIST SOLUTION: THE *LEXMARK* CONCURRENCE

In *Lexmark* and *Chamberlain*, the courts employed a formalist analysis of the text and legislative intent of the DMCA. The central problem in both cases, and in any potential action involving iPhone jailbreaking, is that § 1201's applicability to TPMs that restrict access to hardware is an issue with wide-ranging implications that Congress did not address. Lacking legislative direction, courts face the difficult task of applying and enforcing § 1201 as written without extending the reach of the DMCA further than Congress intended.

In *Lexmark*, Judge Merritt concurred with the majority opinion but offered a different perspective on the problem of determining whether the DMCA should help reinforce software-based hardware lock-ins.<sup>153</sup> Judge Merritt opined that the DMCA cannot be used “in conjunction with copyright law to create monopolies of manufactured goods for themselves just by tweaking the facts of this case.”<sup>154</sup> The concurring opinion emphasized looking to the purpose of the circumvention technology to decide whether or not its aim is to gain access to copyrighted works.<sup>155</sup>

---

151. See iSmashPhone.com, <http://www.ismashphone.com/2008/07/pwnage-tool-20.html> (Jul. 20, 2008 00:40 PST) (demonstrating how to jailbreak your iPhone without unlocking it by not checking the Pwnage tool's “unlock baseband” box).

152. See, e.g., HackThatiPhone.com, [http://www.hackthatphone.com/3x/p\\_3\\_1\\_2\\_3gs.html](http://www.hackthatphone.com/3x/p_3_1_2_3gs.html) (showcasing the “unlock” feature as one of many available for use with the Pwnage tool, the most widely used firmware restore jailbreak).

153. See *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 552 (6th Cir. 2004) (Merritt, C.J., concurring).

154. *Id.* at 551.

155. See *id.*

1. *Problems with the Formalist Approach in the Case of the Apple iPhone*

Although iPhone jailbreaking is likely illegal under *Lexmark* and *Chamberlain*'s formalist approach, the clear intent of the iPhone Software's TPMs is to protect the iPhone itself from tampering. The iPhone Software conducts authenticity checks at every stage of the handset's operation to ensure that the hardware is not used in any way not authorized by Apple.<sup>156</sup> Aftermarket iPhone accessory manufacturers also have to obtain authorization from Apple or run the risk that the next firmware update will render the unauthorized devices incompatible.<sup>157</sup>

Apple has claimed that TPMs are present to ensure the safety of users and wireless networks from viruses and other security problems.<sup>158</sup> While the extent to which iPhone TPMs are necessary is a subject of great debate, it is clear from the design of the iPhone Software's TPMs that Apple made a conscious decision to restrict the hardware in a way that monopolizes its control of the device's aftermarket usage.<sup>159</sup> Under Judge Merritt's functionalist analysis, iPhone jailbreaking is likely not actionable under § 1201.

If courts are to avoid aiding manufacturers in reinforcing aftermarket control of hardware devices and extending the reach of the DMCA, the formalist approach used in *Lexmark* and *Chamberlain* may prove untenable. Both the literal/functional distinction and the "central nexus" tests used in *Lexmark* and *Chamberlain* turn on idiosyncrasies of software design and jailbreaking approach while obscuring the TPM's actual purpose or effects. This is problematic because the literal design of computer code cannot always be strictly correlated with the functional intent of its designer. In fact, the extent to which it can be correlated is often entirely up to the programmer. Ultimately, software designers can decide to code their programs in whatever way they choose. Thus, they may use any programming rationale to justify constructing a TPM that qualifies for protection under a formalist reading of § 1201 protections.

2. *Anti-circumvention Abuse*

Commentators have opined that an uninhibited anti-circumvention right has the potential to lead to anticompetitive economic behavior.<sup>160</sup> Apple's

---

156. See *supra* notes 39–50 and accompanying text.

157. See Apple, Inc., iPhone OS Accessories, <http://developer.apple.com/iphone/program/accessories/> (last visited Jan. 29, 2010); Apple, Inc., Made for iPod Program, <http://developer.apple.com/ipod/> (last visited Jan. 29, 2010).

158. See Response of Apple Inc. at 14, *supra* note 10.

159. See *supra* Part II.

160. See Burk, *supra* note 8, at 1133.

usage of the DMCA to protect its lock-in regimes has drawn similar criticisms.<sup>161</sup> Some commentators have also argued that the DMCA's anti-circumvention right legitimizes a form of technological vigilantism that uses copyright law as a self-help measure to defend its TPMs from reverse engineering.<sup>162</sup> Congress focused on the threat of massive piracy when it composed § 1201 under the DMCA, and therefore this consideration should inform the availability of § 1201 protection. The formalist approach overlooks the protection of digital works as the central rationale behind the DMCA, leaving room for a myriad of unintended applications. In fact, some have argued that many § 1201 cases to date have not been motivated by a fear of piracy but rather a desire to suppress competitive products.<sup>163</sup> *Lexmark*, *Chamberlain* and other aftermarket hardware § 1201 cases support this contention.<sup>164</sup>

As Congress acknowledged during its DMCA discussions, the digital age has given rise to a new generation of progressively more sophisticated and effective copyright pirates. While some applications of § 1201 have indeed targeted piracy or the threat of piracy through trafficking, there are many other instances where § 1201 is used to forcibly modify consumer behavior and practices. To meet the growing threat of piracy, copyright owners and content owners developed increasingly sophisticated TPMs.<sup>165</sup> Not all of these TPMs, however, are directly aimed at preventing piracy. For example, the manifest intent behind DVD region coding, which prevents DVDs purchased in one market from being used in another market, is not piracy prevention but controlling prices and coordinating release dates.<sup>166</sup> Facilitating price discrimination and localization optimizes market control for the global release of DVD content.<sup>167</sup> These mechanisms, while serving to maximize the efficiency and profits for major movie studios, impose a cost on consumers who are prevented from using the content across borders.<sup>168</sup>

---

161. See sources cited *supra* notes 31–38.

162. See Julie E. Cohen, *Reverse Engineering and the Rise of Electronic Vigilantism: Intellectual Property Implications of "Lock-Out" Programs*, 68 S. CAL. L. REV. 1091, 1096–97 (1995).

163. See Burk, *supra* note 9, at 1135–36.

164. See *Sony Computer Entm't Am., Inc. v. Gamemasters*, 87 F. Supp. 2d 976, 981 (N.D. Cal. 1999).

165. See Burk, *supra* note 9 at 1101–02.

166. See Ryan L. Vinelli, *Bringing Down the Walls: How Technology is Being Used to Thwart Parallel Importers amid the International Confusion Concerning Exhaustion of Rights*, 17 CARDOZO J. INT'L & COMP. L. 135, 138; James C. Luh, *Breaking Down DVD Borders*, THE WASHINGTON POST, Jun. 1, 2001 at E01.

167. See Vinelli, *supra* note 157 at 141–42; see, e.g., DVD Copy Control Association, *Frequently Asked Questions*, <http://www.dvcca.org/faq.html> (last visited Jan. 29, 2010).

168. *Id.*

Region coding is in effect a vendor-imposed restriction on consumer behavior; artificially creating a form of market regionalism through technology that cannot be enforced through law.<sup>169</sup>

Technological constraints programmed into an operating system (such as the iPhone Software) provide a self-enforcing substitute for legal ones. For content owners, the choice between legal and technological protections is increasingly evident. Legal protections through contract or licensing may initially be inexpensive, but are ultimately ineffective due to the high cost of bringing suit, both in terms of legal fees and the public relations fallout.<sup>170</sup> Technological protections, on the other hand, may initially be expensive to incorporate and often met with consumer resistance, but are ultimately more effective as consumers become accustomed to them and acquiesce. The introduction of DVD region coding in the early 1990s illustrates this principle. After the DMCA's enactment in 1998, copyright owners and content providers promptly brought suits to reinforce their TPM-backed consumer restrictions.<sup>171</sup>

When a vendor's artificially created restrictions are paired with an anti-circumvention right, content providers gain the ability to legally enforce any technologically supported restriction on consumer behavior—an unwarranted expansion of the DMCA far outside the scope of its drafters' intent.<sup>172</sup> More importantly, this use of the anti-circumvention right erodes consumer choice and is acutely anticompetitive.

Similarly, in the case of the iPhone, Apple depends primarily on the iPhone Software TPMs to maintain and protect its App Store lock-in regime, which would be impractical and ineffective if enforced by law. Unlike the AT&T-Apple contractual lock-in, the Apple App Store lock-in binds the consumer to purchasing apps from Apple by technologically blocking the consumer's ability to use the handset with any other app store platform. By itself, this characteristic could be considered the vendor's prerogative, but

---

169. See Vinelli, *supra* note 166, at 170–71.

170. Similar to the Recording Industry's tactics of suing its consumer base, suing individual jailbreakers may result in user backlash. See Erika Morphy, *RIAA Abandons Mass Lawsuit Strategy in File-Sharing War*, E-COMMERCE TIMES, Dec. 19, 2008, <http://www.ecommercetimes.com/story/65590.html>.

171. See, e.g., *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111 (N.D. Cal. 2002); *Universal Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001); *RealNetworks, Inc. v. Streambox, Inc.*, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. 2000); *Sony Computer Entm't Am., Inc. v. Gamemasters*, 87 F. Supp. 2d 976 (N.D. Cal. 1999).

172. See *supra*, note 61.

when combined with the threats of § 1201 legal action, it is an unjustified abuse of the DMCA's anti-circumvention provisions.<sup>173</sup>

3. *Anticompetitive Effects of the iPhone's Built-In Applications*

iPhone TPMs also lock users into the iPhone's built-in applications (BIA), including streaming video, weather, maps and finance.<sup>174</sup> With one exception, users not content with Apple's BIAs can get the same information supplied by BIAs through Safari, the iPhone's Internet browser, albeit at a significant time cost.<sup>175</sup> Users who want to look up the weather or stock quotes on Safari may sometimes have to wait up to few minutes or more for information that can be obtained in a fraction of the time through the BIAs.<sup>176</sup> This effectively acts as a "soft" lock-in, imposing a high cost on users who choose not to use Apple's BIAs. Moreover, the iPhone Safari web browser cannot play most streaming videos due to its lack of support for the Adobe Flash protocol.<sup>177</sup> In terms of streaming video playback, users have no alternative but to use Apple's YouTube BIA, restricting them to both the BIA and a service provider designated by Apple.<sup>178</sup>

iPhone TPMs and the App Store's own submission process naturally protect iPhone BIAs against competition.<sup>179</sup> iPhone TPMs prevent users from loading custom applications and Apple automatically rejects application submissions it finds duplicative of current and planned features of its BIAs or of the iPhone Software.<sup>180</sup> By monopolizing control of these functionalities on the iPhone, Apple has effectively foreclosed all legitimate opportunities for market competition of these services. Perhaps more troubling is that manufacturers are using this incumbent advantage to shape the users' interactions with the Internet, potentially creating antitrust concerns similar to those raised by the merger of the Windows operating system and Internet Explorer.<sup>181</sup>

Given this potential for abuse, courts should narrow the applicability of § 1201 protections in cases involving aftermarket products and services. This

---

173. See Burk, *supra* note 9, at 1132–1136.

174. See *supra*, note 19.

175. See Ted Landau, *The iPhone needs a faster better Safari*, MAC OBSERVER, May. 14, 2008, [http://www.macobserver.com/tmo/article/The\\_iPhone\\_needs\\_a\\_faster\\_better\\_Safari/](http://www.macobserver.com/tmo/article/The_iPhone_needs_a_faster_better_Safari/).

176. See, e.g., Daring Fireball, <http://daringfireball.net/2009/12/pastrykit> (Dec. 15, 2009).

177. See Brian X. Chen, *Why Apple Won't Allow Adobe Flash on iPhone*, WIRED, Nov. 17, 2008, <http://www.wired.com/gadgetlab/2008/11/adobe-flash-on/>.

178. *Id.*

179. See *supra* note 31 and accompanying text.

180. *Id.*

181. See *United States v. Microsoft Corp.*, 147 F.3d 935, 939 (D.C. Cir. 1998).

would reflect the intent of the DMCA's drafters, who were chiefly concerned with the impact of digital piracy on the market for original works.

4. *The Scope of Section 1201 Anti-Circumvention Should be Narrowed*

To date, numerous commentators have written about § 1201's overreach and many have suggested limiting its scope through legislative reform and judicial discretion.<sup>182</sup> Professor Pamela Samuelson has opined that § 1201 prohibitions "are not predictable, minimalist, consistent, or simple . . . [and] unless the anti-device provisions of the DMCA are modified, either by narrow judicial interpretation or by legislative amendments, they are likely to have harmful effects on competition and innovation in the high technology sector."<sup>183</sup>

To address this problem, this Note proposes a two-part test that requires § 1201 claims to meet the *Chamberlain* central nexus standard and establish a clear causal chain from infringement to market harm. Additionally, courts should focus on the practical effect of the technological measure on consumer choice and competition.

Central to this analysis is a close examination of the original works at issue and the potential for market harm. Per *Chamberlain*, courts should look for a critical nexus between access and protection to determine if the act of circumvention is being used to access actual copyrighted works rather than some auxiliary service or good. Next, courts should examine the exact nature of market harm. In the case of aftermarket goods and services, it is important to assess whether the act of circumvention does in fact violate the copyright owner's rights, creating market harm for the copyrighted work. In order to receive § 1201 protection, plaintiffs must prove that the circumvention of access controls is at least the proximate cause of the market harm to their copyrighted works. This causal chain from circumvention to market harm is necessary to prevent § 1201 protections from being used to reinforce the lock-ins of services or goods that are not protectable under copyright law.

---

182. See, e.g., Haubenreich, *supra* note 26; Jacqueline Lipton, *The Law of Unintended Consequences: The Digital Millennium Copyright Act and Interoperability*, 62 WASH. & LEE L. REV. 487 (2005); Craig Allen Nard, *The DMCA's Anti-Device Provisions: Impeding the Progress of the Useful Arts?*, 8 WASH. U. J.L. & POL'Y 19 (2002); Samuelson, *supra* note 61; Heather A. Sapp, *Garage Door Openers and Toner Cartridges: Why Congress Should Revisit the Anti-circumvention Provisions of the DMCA*, 3 BUFF. INTELL. PROP. L.J. 135 (2006); Pan C. Lee, Daniel S. Park, Allen W. Wang & Jennifer M. Urban, Introduction to the Copyright Reform Act (Prepared on behalf of Public Knowledge), <http://publicknowledge.org/pdf/cra-introduction-02132010.pdf>.

183. Samuelson, *supra* note 61, at 557.

Additionally, in close cases, courts should also look at another factor: the degree to which the original work constrains consumer choice and competition. This will serve as a general-purpose exemption to allow judges to weigh external and market factors in choosing to apply § 1201 protections. In instances where the copyright owners can demonstrate little or no market harm, but are not attempting to control consumer or market behavior, judges may use this additional factor to grant § 1201 protection. Similarly, in cases where the copyright owner can prove market harm, but is using the copyrighted work as gatekeeper to a product or service lock-in regime, judges can choose to withhold § 1201 protection.

This two-step approach prevents vendors and manufacturers from hijacking the DMCA to reinforce their platform lock-ins and limits § 1201 protection to scenarios originally envisioned by Congress. Most importantly, it levels the legal playing field for consumers and new market entrants. Consumer choice is maximized, allowing the end-user to decide whether to incur the cost of breaching contractual lock-ins without the fear of DMCA liability. Taking away legal protection for vendor lock-in regimes also lowers the barrier to entry for new entrants.

All of this comes at a cost to incumbent manufacturer and vendors, who would have to contend with market challengers and competitors on a strictly technological basis. In the event that a vendor chooses to maintain its lock-in regimes, a narrowed application of § 1201 protections may force them to incur additional costs in securing their systems. In the event that market or platform incumbents choose to cooperate with challengers, they must incur the cost of facilitating interoperability to protect the integrity of their existing architecture.

In its current functionality, iPhone jailbreaking is not aimed at replacing or diminishing demand for the iPhone Software in any way. In fact, by opening up its functionality, jailbreaking may potentially make the iPhone more popular and stimulate demand for the iPhone and the iPhone Software. There is also a limited or nonexistent market for the actual copyrighted work being accessed, the iPhone Software, which also happens to be the keystone in Apple's App Store lock-in regime. Under a narrowed application of § 1201, jailbreaking would not be illegal.

## VI. CONCLUSION

For the majority of users, the legality of iPhone jailbreaking will make little or no difference in the purchase and use of iPhone handsets. Apple, by leveraging the power of its incumbency, has attempted to keep widespread

jailbreaking and unlocking at bay by threatening to void the warranties of modified phones.<sup>184</sup> For the most part, Apple's feature-rich App Store and iPhone Software updates have discouraged iPhone modification. Jailbreaking and unlocking both require a basic level of technical expertise and daring. These are obstacles that average users, who are content with the features on their devices, are not incentivized to take on.

However, the Apple iPhone does represent a new class of personal electronics in which the device manufacturer retains control of the only legitimate conduit for new content. Never before has a hardware manufacturer been able to exert so much control over the aftermarket usage of its products. On the iPhone, the iPod and upcoming iPad devices, this control extends to nearly every aspect of the device's features, allowing for little deviation from Apple's prescribed uses. When paired with threats of § 1201 liability, this results in a highly controlled and anticompetitive environment.

Congress never conceived of such a scenario while formulating the DMCA's anti-circumvention provisions, which it crafted to encourage the expansion of freely available digital content on the Internet. Until the legislature addresses the issue, § 1201 protections should be narrowed to ensure they are applied to cases similar to those originally envisioned by Congress and not exploited to the detriment of consumer choice and competition.

---

184. Timothy J. Maun, Comment, *iHack, Therefore iBrick: Cellular Contract Law, The Apple iPhone, and Apple's Extraordinary Remedy for Breach*, 2008 WIS. L. REV. 747, 752 (2008).