

## TEMPTATIONS OF THE WALLED GARDEN: DIGITAL RIGHTS MANAGEMENT AND MOBILE PHONE CARRIERS

NEIL WEINSTOCK NETANEL\*

Content industries have long heralded Digital Rights Management (“DRM”), the use of technological protection to control and meter access to digital content. They view DRM as the key to securing copyrighted expression against massive digital piracy and thus to enabling the industries to distribute their movies, sound recordings, and books in the digital network environment.

Receptive to the content industry call, Congress prohibited the circumvention of such technological protection measures when it enacted the Digital Millennium Copyright Act of 1998 (“DMCA”).<sup>1</sup> It did so with the express purpose of furthering copyright law’s goal of promoting the creation and dissemination of original expression. As the Senate Report accompanying the Act announced, by creating “the legal platform for launching the global digital online marketplace for copyrighted works,” the anti-circumvention provisions sought to “make available via the Internet the movies, music, software, and literary works that are the fruit of American creative genius.”<sup>2</sup>

Yet, ironically, DRM is often used to lock in consumers to ancillary products and services in ways that might hamper markets for distributing cultural expression. Apple’s iTunes is the most widely publicized example. Apple’s combined ACC file format and Fair Play DRM render music and video downloaded from iTunes unplayable on portable media players other than Apple’s iPod.<sup>3</sup> Likewise, Apple’s iPod will not play

---

\* Professor, UCLA School of Law. My thanks to the organizers and participants in the Digital Broadband Migration Conference, February 11-12, 2007, at which I presented an earlier version of this essay. I also thank Talal Shamon and Soichiro Saida for graciously sharing their insights about DRM and mobile carriers, and my research assistants, Lisa Kohn and Wyatt Sloan-Tribe, for their excellent work. All errors are mine.

1. The DMCA provisions are actually both narrower and broader than the summary statement in the text suggests. They are narrower because they do not universally proscribe circumvention of the DRM. They are broader because, in addition to prohibiting circumvention, they prohibit trafficking in devices whose primary design is to enable DRM circumvention. *See infra* notes 26-28 and accompanying text.

2. S. REP. No. 105-190, at 2 (1998).

3. Consumers with the knowledge and time to do so can evade these limitations by burning iTunes music onto a CD in MP3 format and then transferring it to another player. But

proprietary formatted music or video downloaded from online content distribution sites that compete with iTunes (but will play generic MP3s). Apple uses DRM not just to limit unlicensed copying of content, but to anchor its dominance in the market for portable media players and online music distribution. Much to the consternation of the music industry, this puts Apple in the driver's seat in bargaining for licensing terms for music distribution on iTunes.<sup>4</sup> And Apple's DRM-driven defeat of interoperability is blamed by some consumers and technology companies (primarily Apple's rivals) for stifling the growth of the legal digital music download market.<sup>5</sup>

Apple insists that its DRM restrictions have been forced upon it by the record labels and indeed that Apple must maintain a closed proprietary system in order to meet its contractual commitments to the labels to expeditiously remedy any compromise of DRM controls.<sup>6</sup> In that vein, Apple has called upon the recording industry to "abolish DRMs entirely" and has contracted with EMI to distribute a portion of that major label's catalogue free of DRM.<sup>7</sup> However reluctantly, other labels might follow suit.<sup>8</sup>

Commentators sharply disagree on whether Apple truly desires to sell DRM-free music or aims simply to placate consumer advocates and regulatory authorities who have been pressing the company to make the iPod/iTunes system interoperable with other technology platforms.<sup>9</sup> With Apple's June 2007 release of its much touted iPhone, that debate, as well as the debate over interoperability in general, has expanded to the

---

for most users, the Apple limitations are sufficiently burdensome to curtail interoperability.

4. See Yinka Adegoke, *Apple Seen Having Upper Hand in Music Negotiations*, REUTERS, Apr. 20, 2007, <http://www.reuters.com/article/technology-media-telco-SP/idUSN1832165720070423> (noting that the labels are beholden to Apple, which has more than 80 percent of all digital music download sales in the United States).

5. For more on the FairPlay controversy, see Nicola F. Sharpe & Olufunmilayo B. Arewa, *Is Apple Playing Fair? Navigating the iPod FairPlay DRM Controversy*, 5 NW. J. TECH. & INTELL. PROP. 332 (2007). See also Christopher Sprigman, *The 99¢ Question*, 5 J. ON TELECOMM. & HIGH TECH. L. 87, 111-12 (2006) (discussing AAC file format and FairPlay DRM restrictions on interoperability).

6. Steve Jobs states that repairing a leak would be "near impossible if multiple companies control separate pieces of the puzzle, and all of them must quickly act in concert." Apple Inc., *Thoughts on Music*, <http://www.apple.com/hotnews/thoughtsonmusic> (last visited Sept. 26, 2007).

7. See *id.*; see also Brian Garrity, *Adding Up iTunes Plus*, BILLBOARD MAG., June 23, 2007, at 7 (reporting on sales data for DRM-free EMI music on iTunes).

8. See Adegoke, *supra* note 4.

9. *Id.* (reporting the view of "cynical observers" that Apple's call to drop DRM "was sparked by pressure . . . from European regulators to open the iPod/iTunes family to other technology platforms"); see also Ethan Smith & Nick Wingfield, *EMI to Sell Music Without Anticopying Software*, WALL ST. J., Apr. 2, 2007, at B5 (reporting on EMI move, Apple's call to drop DRM, and pressure on Apple by consumer-rights organizations and regulators in several European countries).

mobile carrier arena. Whether due to Apple's contractual obligations or underlying self-interest, Apple and its iPhone partner, AT&T Wireless, have extended and deepened the ACC/FairPlay DRM model. The iPhone and AT&T Wireless subscription agreement follow a proprietary, "walled garden" approach. The iPhone and any iTunes music residing on it may be used and accessed only by AT&T subscribers.<sup>10</sup> And the iPhone may not be used to play proprietary formatted music of iTunes competitors or place phone calls through networks other than AT&T's.<sup>11</sup>

The iPhone is a combined iPod, smartphone, and Internet search device.<sup>12</sup> Each function is hardwired to secure the Apple-AT&T walled garden. In its iPod capacity, the iPhone adopts much the same walled garden functionality as the iPod, with additional restrictions tied to the AT&T subscription. Like the iPod, the iPhone is designed to import music only through the iTunes program on the user's computer and will not play music in rival distributors' proprietary formats. In addition, the iPhone is hardwired to work only if activated by acquiring a two-year cellular subscription with AT&T Wireless, which users initiate when they first connect the iPhone to the iTunes software on their computer.<sup>13</sup> And if the AT&T subscription lapses, the iPhone will no longer work – not as a phone, not as a music and video player, and not as an Internet

---

10. The iPhone is bundled with a two-year subscriber contract with AT&T Wireless, which will be the exclusive carrier of the iPhone at least until 2009. See AT&T Wireless, iPhone Exclusively From AT&T and Apple, <http://www.wireless.att.com/cell-phone-service/specials/iPhoneCenter.html> (last visited Sept. 26, 2007).

11. The applicable AT&T Terms of Service provide: "Equipment purchased for use on AT&T's system is designed for use exclusively on AT&T's system. You agree that you will not make any modifications to the Equipment or programming to enable the Equipment to operate on any other system." Apple Inc., AT&T – Terms of Service, [http://www.apple.com/legal/iphone/us/terms/service\\_att.html](http://www.apple.com/legal/iphone/us/terms/service_att.html) (last visited Oct. 17, 2007). In tandem, Apple's iTunes Terms of Service provide that "[u]se of the Service requires a compatible device" and that "Apple and its licensors reserve the right to change, suspend, remove, or disable access to any Products, content, or other materials comprising a part of the Service at any time without notice." Apple Inc., Apple and Third Party Terms and Conditions, [http://www.apple.com/legal/iphone/us/terms/service\\_all.html](http://www.apple.com/legal/iphone/us/terms/service_all.html) (last visited Oct. 17, 2007).

12. For thorough reviews of iPhone features and restrictions, see Walter S. Mossberg & Katherine Boehret, *Testing Out the iPhone*, WALL ST. J., June 27, 2007, at D1; Kent German & Donald Bell, Review, *Apple iPhone - 4GB (AT&T)*, C/NET, June 30, 2007, [http://reviews.cnet.com/4505-6452\\_7-32180293.html](http://reviews.cnet.com/4505-6452_7-32180293.html).

13. Almost immediately after the iPhone's release, hackers discovered ways to activate the iPhone's web browser and iPod without signing an AT&T contract. But few users will have the technical know-up, or incentive (having spend upwards of \$500 for an iPhone), to do so. See Li Yuan, *Hackers Bypass iPhone Limits*, WALL ST. J., July 6, 2007, at B4. Moreover, Apple responded to the hackers by releasing an iPhone software update that turns unlocked iPhones into functionless "bricks." See Katie Hafner, *Altered iPhones Freeze Up*, N.Y. TIMES, Sept. 29, 2007, at C1. For its part, AT&T has threatened legal action against anyone who offers instruction or tools to unlock the iPhone. See Jennifer Granick, Commentary, *Legal or Not, iPhone Hacks Might Spur Revolution*, WIRED, Aug. 28, 2007, [http://www.wired.com/politics/onlinerights/commentary/circuitcourt/2007/08/circuitcourt\\_0829](http://www.wired.com/politics/onlinerights/commentary/circuitcourt/2007/08/circuitcourt_0829).

search device. At the same time, just as Apple's combined ACC file format and Fair Play DRM renders iTunes content unplayable on rival portable media players, the iPhone and possibly other AT&T handsets, such as the Motorola RAZR V3i, will be the only mobile carrier handsets capable of transferring and housing iTunes music and video from the user's personal computer. The iPhone will sport Wi-Fi and Internet browsing capability. But it will not support downloading Voice-over-IP clients such as Skype, so it will be capable of making and receiving telephone calls only through the AT&T cellular network.

The Apple-AT&T walled garden approach, in short, employs a combination of DRM and proprietary format to attract and then lock in consumers to the iPhone and AT&T subscription. Consider a consumer who purchases an iPhone and signs up for a two-year AT&T contract. At the very least, the consumer is locked in to the AT&T service for the two years of the contract.<sup>14</sup> That is already common practice for mobile telephone service. What Apple adds is an additional layer of stickiness at the end of the contract. The consumer who moves to another carrier will no longer be able to use her iPhone. She will not only require her new carrier's handset to engage in cellular communications; she will also lose the ability to use the iPhone as an Internet search device and media player. If she wants to continue to play her iTunes content on a mobile device, she will have to purchase an iPod.<sup>15</sup>

While the iPhone and iTunes will be available exclusively for AT&T subscribers, AT&T provides music, video, and games from other sources for use on other handsets as well. AT&T is not alone. Mobile carriers are rapidly becoming multimedia data portals and distributors. In most countries, markets for basic cellphone service are becoming saturated. As a result, wireless carriers and handset manufacturers are racing to develop technologies and business models for some combination of streaming and downloads of videos, live TV programming, music, web browsing, multiplayer gaming, social networking, and information, such as GPS, local traffic reports, and weather conditions, tailored to people on the go.<sup>16</sup> Like the iPhone, in

---

14. AT&T's Terms of Service provide that a customer who terminates the service prior to expiration of the two-year period must pay a termination fee in the amount of \$175 for each wireless telephone number associated with the service. AT&T – Terms of Service, *supra* note 11.

15. XM satellite radio follows a similar model for its mobile player device, the Inno; songs recorded from XM radio onto the Inno can no longer be accessed if the XM radio subscription lapses (or indeed if the Inno fails to receive at least 8 hours of live XM radio signal per month in order to authenticate the user's subscription). See PIONEER ELECS. SERV., INC., INNO USER GUIDE 26 (2006), available at [http://www.xmradio.com/pdf/hardware\\_support/pioneer/inno/userguide.pdf](http://www.xmradio.com/pdf/hardware_support/pioneer/inno/userguide.pdf).

16. J.A. Harmer, *Mobile Multimedia Services*, BT TECH. J., July 2003, at 169; Li Yuan, *Cellphone Video Gets on the Beam*, WALL ST. J., Jan. 4, 2004, at B3.

short, cell phones are metamorphosing into multi-purpose, multi-media communications, information, content player, and content receiver devices. Industry analysts predict that mobile content and entertainment revenues will grow exponentially in Europe and the United States over the next several years, with U.S. revenues reaching \$50 billion by 2010.<sup>17</sup>

The Apple-AT&T walled garden approach to locking in consumers (or at least erecting barriers to consumer mobility) might be attractive for other mobile carriers as well.<sup>18</sup> Mobile communications carriers have long sought to combat customer churn. They have used a variety of devices to do so, including long-term subscriber contracts, deploying DRM to lock handsets so the handset cannot be used with a different carrier, and requiring consumers to change their telephone number when moving to a new carrier. Churn rates have declined over the past year or two, whether because of the success of these tools (other than that of requiring consumers to change their telephone numbers, since the FCC now requires number portability), greater consumer satisfaction with existing carriers, or industry consolidation and its resulting reduction in competition.<sup>19</sup> Nevertheless, churn rates remain high, reportedly resulting in a loss of between 18 and 36 percent of subscribers each year.<sup>20</sup> Applying DRM to condition subscribers' access to music, video, and other content upon their continued use of the carrier's service presents yet another tool for combating subscriber churn.

To a certain degree, the leading carriers already use DRM to tether content to their service. When subscribers move to a new carrier they typically lose any ringtones, video, music, or games they downloaded onto their handset because their handset cannot be used with the new carrier. The carriers do sometimes enable subscribers to move downloaded content from their handset to their computers in a standard format. The Verizon V-Cast and Sprint Digital Lounge music services, for example, allow subscribers to transfer downloaded music from their handsets to their computers in Windows Media format. Handsets can

---

17. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, DIGITAL BROADBAND CONTENT: MOBILE CONTENT - NEW CONTENT FOR NEW PLATFORMS 9 (2005), <http://www.oecd.org/dataoecd/19/7/34884388.pdf>.

18. Cf. CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 109-10 (1998) (discussing strategies to deter customer mobility by imposing switching costs); see also Robert Cyran & Edward Hadas, *Learning From Palm's Pain*, WALL ST. J., Mar. 6, 2007, at C2 (contending that consumer technology firms in general would do better to build "sticky features" into their products to give consumers a disincentive to switch to rival devices).

19. Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, *Report*, 21 Fcc Rcd. 10,947, 11,011-13 (2006), available at [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/FCC-06-142A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-142A1.pdf) [hereinafter FCC 2006 Mobile Services Report].

20. *Id.*

also be designed to store content obtained from third parties, much like MP3 players. In these instances, the use of DRM to render handsets incompatible with other carriers is more a hindrance than a significant barrier to moving to a new mobile carrier. While a subscriber who leaves Verizon or Sprint must typically obtain a new handset for his new carrier, he can still transfer music from his computer to his new handset, so long as it is Windows Media compatible.

Mobile carriers, in short, have a variety of technological and market options for using DRM to erect a walled garden and tether content to their services as a means of locking in consumers. (I realize that “lock-in” is overstating. I mean it as a shorthand for creating greater stickiness, imposing a cost on consumer mobility, not an absolute barrier.). The use of DRM to combat mobile subscriber churn is quite different, and may have different regulatory implications, from DRM’s use to protect content against copyright infringement. This paper entertains the possibility that mobile carriers will follow the Apple-AT&T walled garden approach. It considers the regulatory implications of mobile carriers’ design and use of DRM to lock in their subscribers as opposed to deploying DRM to protect rights in the content itself by preventing the music and video that subscribers purchase from leaking out into unlicensed peer-to-peer file trading networks. AT&T has already threatened legal action against those who offer instructions or tools to unlock the iPhone.<sup>21</sup> How does and should the law view the Apple-AT&T use of DRM to enforce their iTunes/iPhone/AT&T network walled garden and others’ efforts to break down the walls by hacking the iPhone and FairPlay DRM?

I first consider whether consumers would and should be able to circumvent such DRM under the DMCA. Does a mobile carrier’s use of DRM to lock in consumers to its service serve the goals of the DMCA? In answering that question, should it matter whether the carrier deploys DRM on copyrighted content as opposed to using DRM simply to lock the handset? And under judicial interpretation of the DMCA, would circumvention for the limited purpose of being able to move to a new carrier and still access content the consumer purchased from his prior carrier violate the anti-circumvention proscriptions of the Act? I then consider mobile carriers’ use of DRM to lock in consumers from the telecommunications regulation perspective. The FCC mandated number portability, but refused to ban handset locks. How might it regard and how should it regard content mobility under current market conditions?<sup>22</sup>

---

21. For discussion of AT&T’s threatened legal action, *see* Granick, *supra* note 13.

22. I do not consider a possibly relevant third legal regime: claims by consumers against mobile phone manufacturers or carriers who deploy DRM to disable a handset or service in response to the consumer’s unlocking of the handset. A class action lawsuit recently filed



Before I proceed, I want to clarify: it is by no means a foregone conclusion that mobile carriers will follow the walled garden approach rather than one that allows for interoperability. Markets for digital distribution of content are in great flux and mobile carriers stand at a crossroads regarding their business model for multimedia content distribution, choice and application of DRM, and selection of strategic partners. On one hand, using DRM to establish a proprietary, branded content distribution network, and to lock in subscribers at the same time, offers the potential to capture substantial rents. Apple has done very well with its iTunes/iPod model by creating a high quality, user friendly, attractively branded end-to-end experience. But on the other hand, consumers want interoperability. They want to be able to seamlessly transport content and applications from one device and service to another. Apple's proprietary model for computers did not fare so well against the greater interoperability of the Windows/PC platform.

Industries typically seek some element of proprietary product and branding. No firm wants to compete in a fully commodified market if that can be avoided. In these early days of entering the multimedia content distribution market, mobile carriers have yet to determine the extent to which deploying DRM to help secure their proprietary networks is a viable long-range option.

The Open Mobile Alliance's DRM standard reflects that ambivalence. The Open Mobile Alliance is a telecommunications, information technology, and content industry umbrella organization, with the stated mission "to facilitate global user adoption of mobile data services by specifying market driven mobile service enablers that ensure service interoperability across devices, geographies, service providers, operators, and networks, while allowing businesses to compete through innovation and differentiation."<sup>23</sup> The Alliance, which counts the leading mobile carriers (as well as handset manufacturers and IT companies) among its members and sponsors, has released a DRM specification called OMA 2.0 for use in mobile handsets and other consumer electronics devices.<sup>24</sup> OMA 2.0 is designed to enable content providers,

---

against Apple alleges that Apple's extrajudicial enforcement of the iPhone-AT&T Wireless bundle through iPhone software updates that render unlocked iPhones into functionless "bricks" violates California antitrust and unfair competition law. *See* Complaint for Treble Damages and Permanent Injunctive Relief, *Smith v. Apple Inc.*, No. 1-07-CV-095781 (Cal. Super. Ct. Oct. 5, 2007), *available at* [http://www.appleiphonelawsuit.com/uploads/Class\\_Action\\_Complaint\\_Smith\\_vs\\_Apple.pdf](http://www.appleiphonelawsuit.com/uploads/Class_Action_Complaint_Smith_vs_Apple.pdf).

23. Open Mobile Alliance, <http://www.openmobilealliance.org/> (last visited Sept. 27, 2007).

24. *See* Open Mobile Alliance, OMA Release Program and Specifications, [http://www.openmobilealliance.org/release\\_program/drm\\_v2\\_0.html](http://www.openmobilealliance.org/release_program/drm_v2_0.html) (last visited Sept. 27, 2007).

mobile carriers, and others to wrap content to enable consumers to transport content across several registered devices. But it also enables a provider or mobile carrier to place obstacles to interoperability and transportability.<sup>25</sup>

## I. DIGITAL MILLENNIUM COPYRIGHT ACT

With the advent of digital technology and the Internet, copyright industries faced the threat of massive unlicensed copying and distribution of their copyrighted works. In response, the industries began to deploy technological protection measures, including digital encryption, to control access to and copying of their content. Enacted in 1998, the Digital Millennium Copyright Act (“DMCA”) neither mandates nor restricts the use of such technological protection measures (which have come to be called Digital Rights Management (“DRM”), inaccurately because they can be used to secure content and services beyond the scope of any preexisting legal “rights”). Rather, the DMCA contains far-reaching provisions designed to combat the circumvention of those technological protection measures that are deployed to control access to or uses of copyrighted content.

The DMCA’s anti-circumvention provisions are of two basic types. First, the DMCA prohibits users from circumventing technology that controls access to protected works.<sup>26</sup> Second, the Act prohibits the manufacture and trafficking of devices, technology, and services that are primarily designed to assist users in circumventing technology that (1) controls access to content that is protected under the Copyright Act,<sup>27</sup> or (2) effectively protects a copyright holder right by controlling uses of such content.<sup>28</sup>

---

25. It is sometimes said that DRM, by its very nature, must impose some limits on interoperability and transportability. As one knowledgeable observer states:

‘[T]ruly interoperable DRM’ . . . is a fallacy. By definition, there is no such thing, nor can there be. The whole point of DRM is being able to control the use and distribution of content. . . . If the DRM restrictions were too liberal, then the music files could be easily shared. That would obviously defeat the purpose of using DRM in the first place.

Technical Conclusions, <http://technicalconclusions.wordpress.com/2007/02/22/thoughts-on-drm-part2/> (Feb. 22, 2007) (blog posting titled Thoughts on DRM: Part II). The idea that DRM means limits on interoperability may well be true for DRM that aims to control the use and distribution of content. But it does not hold for DRM that aims only to meter uses on any device on which the content is used, for purposes of extracting payment from the user or a third party, such as the device or service provider or an advertiser. See Neil Weinstock Netanel, *Impose a Noncommercial Use Levy to Allow Free Peer-to-Peer File Sharing*, 17 HARV. J.L. & TECH. 1 (2003) (presenting a blueprint for using DRM to meter, but not control, personal, noncommercial uses of digital content).

26. 17 U.S.C. § 1201(a)(1)(A) (2000).

27. See *id.* § 1201(a)(1)(E).

28. See *id.* § 1201(b).



As the Second Circuit has put it, in outlawing the circumvention of access controls and prohibiting circumvention devices, “Congress sought to combat copyright piracy in its earlier stages, before the work was even copied.”<sup>29</sup> Others have posited that even though copyright law does not accord copyright owners with an exclusive right to control access to their works, the DMCA’s access prohibition provides the legal framework for copyright holders to market various forms of access, ranging from streaming to pay-per-use, as an alternative to selling permanent copies.<sup>30</sup> In that way, copyright industries will be able to charge differential prices tailored to consumer demand, and consumers will correspondingly have the option of buying access to content on a subscription model or paying for a one-time viewing or listening rather than purchasing a permanent download.

At the same time that it provided legal support for a pay-per-use business model, Congress expressed concern that pay-for-use might run amok, that it might ultimately reduce, rather than enhance, access to “copyrighted materials that are important to education, scholarship, and other socially vital endeavors.”<sup>31</sup> Congress particularly feared the “perfect storm” combination of the elimination of print or other hard-copy versions, permanent encryption of all electronic copies, and adoption of business models that restrict distribution and availability of works.<sup>32</sup> To address that concern and “maintain balance between the interests of content creators and information users,” Congress delegated to the Librarian of Congress the power to suspend application of the access prohibition to the extent and duration required to prevent “a diminution in the availability to individual users of a particular category of copyrighted materials,” particularly for favored, productive uses such as scholarship, education, criticism, and news reporting.<sup>33</sup> The Act provides for a Library of Congress rulemaking every three years so that the Librarian can determine, upon the recommendation of the Register of Copyrights (who must consult with the Assistant Secretary for Communications and Information of the Department of Commerce), whether the prohibition adversely impacts persons’ “ability to make non-infringing uses under this title of a particular class of copyrighted works.”<sup>34</sup> If the Librarian finds such adverse impact, the prohibition does not apply to “such users with respect to such class of works for the

---

29. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 435 (2d Cir. 2001).

30. See Jane Ginsburg, *From Having Copies to Experiencing Works: the Development of an Access Right in U.S. Copyright Law*, 50 J. COPYRIGHT SOC’Y 113 (2003).

31. H.R. REP. No. 105-551, pt. 2, at 36 (1998).

32. *Id.*

33. *Id.* at 35-36; 17 U.S.C. § 1201(a)(1)(C).

34. 17 U.S.C. § 1201(a)(1)(C).

ensuing 3-year period.”<sup>35</sup>

The Library of Congress rulemaking and case law applying the DMCA both impact the extent to which mobile subscribers may lawfully circumvent mobile carriers’ DRM. I consider each in turn.

#### A. *Library of Congress Rulemaking*

In his November 2006 rulemaking, the Librarian exempted from the access prohibition “[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>36</sup> In promulgating the three-year, possibly renewable exemption, the Librarian found that the handset “access controls do not appear to actually be deployed in order to protect the interests of the copyright owner or the value or integrity of the copyrighted work; rather, they are used by wireless carriers to limit the ability of subscribers to switch to other carriers, a business decision that has nothing whatsoever to do with the interests protected by copyright.”<sup>37</sup> As of November 2006, therefore, consumers and others may unlock a handset in order to enable its use for wireless communication through a new mobile carrier.

It is easy to see why carriers lock handsets to reduce subscriber churn. A locked handset imposes an immediate cost on a subscriber who wishes to switch carriers: the subscriber must buy a new handset and spend the time to personalize it by entering contact lists and the like. In addition, the subscriber loses any content – music, videos, and photographs – that are stored on the locked handset. At a minimum, the subscriber must retrieve and transfer copies of that content from the subscriber’s PC to her new handset. And depending on circumstances and any DRM limitations imposed on the content itself, the subscriber might simply lose the sunk cost of purchasing it through her previous carrier.

The Library of Congress rule might appear to greatly undermine mobile carrier efforts to combat churn through locking handsets. Most obviously, the exemption makes it possible for subscribers to save the costs of purchasing a new handset and re-inputting personal information. In addition, if subscribers can take their old handsets with them, they might also be able to continue to access whatever downloaded content

---

35. *Id.* § 1201(a)(1)(D).

36. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68,472, 68,476 (Nov. 27, 2006) (to be codified at 37 C.F.R. pt. 201) [hereinafter Librarian Rulemaking].

37. *Id.*

that resides on that handset. In that event, carriers could not combat subscriber churn by selling content to subscribers for download to their handsets and then using handset locks to prevent subscribers from subsequently unbundling the content from their subscriptions.

For a couple reasons, however, the November 2006 rule may have a lesser import than might otherwise seem. First, the rule does not prohibit mobile carriers from continuing to use DRM to lock their handsets, and U.S. mobile carriers show no signs of discontinuing the practice.<sup>38</sup> The rule simply permits reprogramming the handset to use it on a different network. That means that the subscriber must still obtain the knowledge or tools to reprogram the handset or find someone to do it for him. As is apparent from Apple's highly effective use of DRM-laden software updates to render unlocked iPhones into entirely functionless "bricks," that can be no easy task.<sup>39</sup> Moreover, the Librarian of Congress has the authority to suspend just the prohibition on circumvention itself. It remains a violation of the DMCA to provide a "technology, product, service, [or] device . . . that is primarily designed or produced for the purpose of circumventing" an access control measure.<sup>40</sup> Thus, assuming that handset locks in fact qualify as measures that control access to copyrighted works under the DMCA – and we will shortly see how questionable that proposition might actually be – websites that feature handset unlocking software would continue to run afoul of the DMCA trafficking prohibition even if the Librarian rulemaking now permits users to unlock. The same might apply to any mobile carrier or third party that provides the service of unlocking handsets to enable a subscriber to use her handset on a new network.

Second, the Librarian distinguished between circumventing to use a handset on the network of the customer's choosing and circumventing to gain unauthorized access to copyrighted content. As the rulemaking notes, "owners of copyrights in music, sound recordings and audiovisual works whose works are offered for downloading onto cellular phones . . . expressed concern that the proposed exemption might permit circumvention of access controls that protect their works when those works have been downloaded onto cellular phones."<sup>41</sup> The Librarian found that "[t]he record on this issue was fairly inconclusive" and thus,

---

38. See Marguerite Reardon, *Will Unlocked Cell Phones Free Consumers?*, C/NET NEWS.COM, Jan. 24, 2007, [http://news.com.com/Will+unlocked+cell+phones+free+consumers/2100-1039\\_3-6152735.html](http://news.com.com/Will+unlocked+cell+phones+free+consumers/2100-1039_3-6152735.html) (noting that while a few retailers are beginning to see unlocked handsets, the major mobile carriers continue to limit their subscribers to the locked handsets that the carrier sells).

39. See Hafner, *supra* note 13.

40. See 17 U.S.C. § 1201(a)(2).

41. Librarian Rulemaking, *supra* note 36, at 68,476.

in essence, that he need not address the issue head-on.<sup>42</sup> He granted the exemption on the assumption that it was “sought for the sole purpose of permitting owners of cellular phone handsets to switch their handsets to a different network,” not gain unauthorized access to content.<sup>43</sup>

The Librarian’s rule and explanation do not fully answer the question of whether it violates the DMCA to circumvent a carrier’s lock on a content-laden handset to enable the subscriber *both* to use the handset with a new carrier *and* continue to have access to the content on the handset. Does the answer depend on the subscriber’s primary motive? Or is it the carrier’s primary motive – to use DRM to combat subscriber churn as opposed to control access to copyrighted content per se – that matters? Might the Librarian rule differently in three years if carriers and content providers introduce into the record clear evidence that unlocking handsets provides continued, unauthorized access to content residing on the handset?

The Register of Copyright’s recommendation to the Librarian to issue the handset lock exemption does little to elucidate this issue. The Register found that copyrighted content can be protected by DRM access controls that are separate from those that lock the handset itself. It noted, indeed, that “the Open Mobile Alliance standard, ‘places DRM functionality at a different layer than Service Provider functionality,’ and that the ‘content industry, in collaboration with the carriers and manufacturers, can simply choose to store the keys to DRMed audiovisual material elsewhere, as is currently the case with many of the handsets on the market.’”<sup>44</sup> The Register also suggested that “a prudent copyright owner of works offered for download to wireless telephone handsets would be wise to insist that access to those works be protected by access controls other than those which control access to the part of the firmware that governs with which wireless communication network the handset will communicate.”<sup>45</sup>

However, the Register stopped short of concluding that content providers who rely on the carrier’s handset lock, rather than deploying distinct access controls narrowly targeted to their content only, thereby forfeit protection under the DMCA access prohibition. The Register, rather, based her recommendation for the exemption for circumventing

---

42. *Id.*

43. *Id.*

44. Letter from Marybeth Peters, Register of Copyrights, to James H. Billington, Librarian of Congress 53 (Nov. 17, 2006) (quoting the oral comments of Jennifer Granick, Stanford Law School, Center for Internet and Society’s Cyberlaw Clinic, on behalf of The Wireless Alliance and Robert Pinkerton), *available at* [http://www.copyright.gov/1201/docs/1201\\_recommendation.pdf](http://www.copyright.gov/1201/docs/1201_recommendation.pdf) [hereinafter Copyright Register 2006 Recommendation].

45. *Id.* at 53 n.157.

handset locks on the absence of evidence in the record that handset locks actually control access to content. As her recommendation stated, “because it appears that there is no reason why those other works cannot be protected by separate access controls, there is no justification for denying an exemption based on speculation that the exemption might permit circumvention that would remove restrictions on access to those works.”<sup>46</sup> And the Register recommended tailoring the exemption “so that it does not allow circumvention in order to gain access to copyrighted works, uses of which have not been shown to be noninfringing,” suggesting that the exemption should not be available where the handset lock is, in fact, designed to control access to content residing on the handset, whether as a central feature as in the case of iPhone or merely as an intended byproduct of preventing the handset’s use in a competing telecommunications network.<sup>47</sup>

The Librarian’s rulemaking and Register’s recommendation make it clear that the exemption for unlocking handsets does not apply to any DRM that carriers might use to lock content itself, separately from, or in addition to, the handset lock. The 2006 exemption would be unavailable, for example, to circumvent DRM that follows the Apple-AT&T regime of blocking access to content if the mobile handset owner no longer has a subscription with the carrier.

Should such circumvention be otherwise exempted from the DMCA’s access prohibition? Say the mobile carrier deploys DRM following the OMA 2.0 standard and configures it not only to protect the content against unauthorized copying, but also to limit its subscribers’ ability to switch to other carriers by rendering the content inaccessible upon termination of the bundled subscription. Would and should the Librarian of Congress view that latter use of DRM, like the carriers’ handset locks, to reflect “a business decision that has nothing whatsoever to do with the interests protected by copyright?”<sup>48</sup> Does mobile carriers’ use of DRM on copyrighted content as a means to combat subscriber churn, over and above protecting the content against unlicensed copying and public distribution, serve the DMCA’s purpose of promoting the availability in digital form of “the movies, music, software, and literary works that are the fruit of American creative genius[?]”<sup>49</sup>

In its DMCA rulemaking recommendations, the Register of

---

46. *Id.* at 53.

47. *Id.* The Register takes what I believe is the correct position that a technological feature or format that inadvertently impedes access does not constitute a “technological protection measure that effectively controls access to a work” within the meaning of the DMCA. Rather the technological impediment must be “imposed in order to control access to a work.” *Id.* at 33.

48. Librarian Rulemaking, *supra* note 36, at 68,476.

49. S. REP. No. 105-190, *supra* note 2, at 2.

Copyrights has thus far soundly rejected arguments that consumer circumvention to engage in “space-shifting” of content across devices and formats, such as moving movies from DVDs to one’s iPod or moving iTunes music to a non-iPod MP3 player, should be exempted from the access prohibition.<sup>50</sup> In so concluding, the Register has found that exemption proponents have failed to demonstrate that such space-shifting is fair use (which would weigh in favor of an exemption but would not be determinative).<sup>51</sup> The Register has opined, indeed, that “[c]ertainly, where the [unauthorized] online distribution of works is a potential concern, space-shifting will be incompatible with fair use.”<sup>52</sup> Supporting that view, the Register has found that DRM tethering of copyrighted works to particular devices and distribution channels has in fact served to guard against the risk of massive illegal distribution and thus promoted greater legal distribution and availability of copyrighted works in digital form.<sup>53</sup>

However, mobile carriers’ use of DRM to combat subscriber churn, rather than protect content against piracy, seems distinguishable. Likewise, so does subscribers’ circumvention of that DRM to continue to have access to content that the subscriber has purchased and that resides on the subscriber’s handset, rather than to space-shift that content to a new device. Almost by definition, this use – and circumvention – of DRM seem to have little to do with interests protected by copyright and everything to do with mobile carriers’ communications service business models.

Or do they? As markets and content distribution channels converge, mobile carriers become as much content distributors as providers of telephony and other personal communications services. At some point, their use of DRM to retain subscribers has as much to do with copyright as similar uses by any other content distributor. These include the iPod and iPhone models, as well as the XM Radio/Inno model, under which downloaded music can no longer be accessed when the Inno owner’s XM Radio subscription has ceased. They also include the Napster subscription download service whereby, similarly, music downloaded as

---

50. See Copyright Register 2006 Recommendation, *supra* note 44, at 69-72.

51. *Id.* at 70. The DMCA provides that nothing in the anti-circumvention provisions “shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.” 17 U.S.C. § 1201(c)(1). But that provision stops short of providing a fair use defense to circumvention in violation of the provisions themselves and the Librarian is not required to exempt any uses that are fair uses, but only particular classes of *works* for which the circumvention prohibition adversely impacts persons’ ability to make noninfringing uses. *Id.* § 1201(a)(1)(C).

52. *Id.* at 71 (quoting Letter from Marybeth Peters, Register of Copyrights, to James H. Billington, Librarian of Congress 32 (Oct. 27, 2003), available at <http://www.copyright.gov/1201/docs/registers-recommendation.pdf>).

53. Copyright Register 2006 Recommendation, *supra* note 44, at 71.



part of the Napster subscription is no longer playable if the subscription expires, as well as a host of other subscription services, ranging from online music to cable television, which cease providing access to provider supplied content once the subscription ceases.

DRM access controls in these cases make it possible for content distributors to offer content in various forms and prices. Napster, for example, also sells downloads that purchasers are entitled to keep and play even if they cancel their Napster subscription. These uses of DRM might not aim to prevent unauthorized copying per se; they are access controls, not copy controls. Yet the business models they make possible arguably serve as an incentive for content distributors of various stripes to make digital content more widely available. At least that is an empirical question, and one that touches upon the Librarian's DMCA rulemaking: whether the deployment of DRM is enhancing or impeding socially valuable access to a given category of works. But in a future world in which wireless communications and copyrighted content distribution are integrated within the same markets and services, it should probably not matter for that calculus whether the content distributor is Verizon, Apple, Napster, or Disney.

#### *B. DMCA Case Law*

Case law under the DMCA supports a similar conclusion. Manufacturers have used technological protection measures to prevent competition in the aftermarket for spare parts and other related goods and services, ranging from garage door openers to ink cartridges. The technology typically involves software code on interoperating parts that must effect a "handshake" in order for the parts to work with one another. Competitors have in turn devised code to mimic or circumvent that handshake barrier, and some have been sued for circumventing an access control under the DMCA.

The manufacturers have met with little success in these lawsuits; courts have repeatedly found ways to hold that the DMCA does not apply to protect exclusivity in aftermarkets for consumer goods in which manufacturers have embedded computer code. In *Chamberlain Group, Inc. v. Skylink Technology, Inc.*, for example, the Federal Circuit held that the DMCA "prohibits only forms of access that bear a reasonable relationship to the protections that the Copyright Act otherwise affords copyright owners."<sup>54</sup> The DMCA, the court stated, was designed to "bring copyright law into the information age," and in so doing, to "maintain balance between the interests of content creators and

---

54. *Chamberlain Group, Inc. v. Skyline Techs., Inc.*, 381 F.3d 1178, 1202-03 (Fed. Cir. 2004).

information users.”<sup>55</sup> The anti-circumvention provisions, the court noted as well, were aimed to implement the World Intellectual Property Organization Copyright Treaty, which requires countries to prohibit “the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights” under copyright treaties.<sup>56</sup> The DMCA applies only when unauthorized access would infringe or facilitate infringement of a copyright. It does not enable a manufacturer to retract consumers’ prerogative to use a copy of embedded software in a product they purchased.<sup>57</sup>

A year later, the Federal Circuit declined to extend the DMCA to prevent circumvention of software protection measures designed to provide the plaintiff exclusivity in providing maintenance and repair services for a computer data storage and retrieval system. In so doing, the court reiterated that when “rights under copyright law are not at risk, the DMCA does not create a new source of liability.”<sup>58</sup> And, likewise, the Sixth Circuit held that the authentication sequence that a printer manufacturer had embedded in its ink cartridges did not “control access” to the code in the printer and thus could be circumvented without running afoul of the Act.<sup>59</sup>

Applying that precedent, it seems fairly clear that the Librarian of Congress probably did not have to provide an exemption for circumventing handset locks. Circumventing a handset lock that serves only to prevent a mobile phone subscriber from moving to a new network would unlikely be held to violate the DMCA in any event. Like the authentication sequences designed to maintain exclusivity in aftermarket goods and services, mobile carriers’ handset locks aim to lock in customers to a business, not protect copyrights or expressive content.

But what if the handset lock served the dual purpose of combating subscriber churn *and* controlling access to copyrighted music, video, and pictures residing on the handset? Or what if the mobile carrier uses the technological control over access to content as an additional means of locking in subscribers? And what if the carrier does so despite the ready availability of DRM that more narrowly protects content against unlicensed copying and distribution when the subscriber moves to a new carrier (something along the lines contemplated by the OMA 2.0 transportability function)? Would the Federal Circuit then view the

---

55. *Id.* at 1196-97.

56. *Id.* at 1194.

57. *See id.* at 1203.

58. *Storage Tech. Corp. v. Custom Hardware Eng’g & Consulting, Inc.*, 421 F.3d 1307, 1318 (Fed. Cir. 2005).

59. *Lexmark Int’l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 546-47 (6th Cir. 2004).

carrier's use of DRM as one that bears insufficient relation to preventing copyright infringement?

The cases suggest that courts do not require content providers to narrowly tailor their DRM in such a manner. In *Universal City Studios, Inc. v. Corley*, for example, the defendants argued that the software they provided to circumvent the CSS protection on movie DVDs was designed only to enable users of the Linux operating system to play DVDs that they had legitimately purchased. The district court found that contention "immaterial" even if accurate.<sup>60</sup> In upholding the district court's ruling, moreover, the Second Circuit noted that the defendants "offered no evidence that the Plaintiffs have either explicitly or implicitly authorized DVD buyers to circumvent encryption technology to support use on multiple platforms."<sup>61</sup> For the Second Circuit, evidently, the movie studios have the absolute prerogative to use technological protection measures that restrict viewing DVDs to computers with Windows or Apple operating systems, presumably even if Linux compatible DRM were readily available.

In like vein, the Eighth Circuit held in *Davidson & Associates v. Jung* that operators of a website platform for users of Blizzard Entertainment video games to play those games in a multi-player environment without using Blizzard's official multi-player website had violated the DMCA.<sup>62</sup> The defendants were a group of non-profit volunteer game hobbyists, programmers, and others who established their alternative site for playing Blizzard games out of frustration with inadequacies in Blizzard's proprietary site. Significantly for the DMCA claim, Blizzard's official website was constructed to require an authentication sequence "handshake" between an authorized copy of a Blizzard game and the website server in order for the user to enter the site. The defendants' site did not require that "handshake." It automatically allowed all games to be played regardless of whether a game correctly completed the handshake. The Eighth Circuit did not explain how the defendants had thereby circumvented a technological protection measure that controlled access to the plaintiffs' copyrighted games. It did note that the defendants' lack of a requirement that games complete the official "handshake" made it possible for users of illicit copies to play the game in the defendants' multi-player environment.<sup>63</sup> But that did not seem to be the defendants' intention and, in any event, does not mean that the defendants violated the DMCA.

Importantly for our discussion, the defendants reportedly had

---

60. *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 319 (S.D.N.Y. 2000).

61. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 444 (2d Cir. 2001).

62. *Davidson & Assocs. v. Jung*, 422 F.3d 630, 642 (8th Cir. 2005).

63. *Id.* at 640.

offered to implement an authentication process for their servers to prevent entry to users of illicit copies of Blizzard games.<sup>64</sup> But Blizzard rejected that offer, insisting that it needed to keep its authentication sequence secure.

The *Universal* and *Davidson & Associates* decisions suggest that the DMCA access and trafficking prohibitions will apply even when (1) the defendant circumvents or enables others to circumvent solely to use legitimate copies of copyrighted material on a platform for which the DRM was not designed and (2) the copyright holder could have designed the DRM to be compatible with that platform but chose not to, so long as (3) there is some nexus between the DRM and protecting copyrights. If that reasoning is applied in the mobile carrier arena, it seems that mobile carriers and their copyright holder licensees could use the DMCA to prevent circumvention of DRM that has the effect of locking in subscribers to a particular carrier so long as the DRM also protects copyrighted content from possible illicit copying and distribution. The failure of the mobile carrier and licensee to narrowly target the DRM to prevent only unlicensed copying and distribution, but still allow the subscriber to access purchased content from his or her new mobile communications network, would not give rise to a privilege to circumvent, even solely for the purpose of switching networks. Apple-AT&T could not use the DMCA to prevent subscribers from bypassing a handset lock to use their iPhones on another cellular network. But they could invoke the DMCA against those who seek to hack around whatever DRM software disables the iPhone from accessing iTunes content if the owner's AT&T subscription expires.

## II. FEDERAL COMMUNICATIONS COMMISSION

The Federal Communications Commission has the authority to forbid mobile carriers from using DRM to lock in subscribers. Under the Telecommunications Act of 1996, the FCC regulates (or decides not to regulate) to “promote competition and . . . secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies.”<sup>65</sup> The Commission has previously acted to promote competition among telecommunications service providers by mandating number portability. But the Commission declined to prohibit mobile carriers from bundling handsets with service contracts.

---

64. A.H. Rajani, Note, *Davidson & Associates v. Jung: (Re)interpreting Access Controls*, 21 BERKELEY TECH. L.J. 365, 374 (2006).

65. These goals are set forth in the Preamble to the Act. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 15, 18, and 47 U.S.C.).

The FCC considered carriers' bundling of handsets with service contracts in 1992.<sup>66</sup> The Commission conducted its inquiry in light of the prevalent practice of mobile carriers requiring customers to purchase their handsets directly from the carrier or an authorized carrier agent and to contract to pay for a minimum amount of wireless airtime per month over a period of a year or more. In its ruling, the Commission expressed "concern that customers have the ability to choose their own CPE [handset] and service packages to meet their own communications needs and that they not be forced to buy unwanted carrier-provided CPE [handsets] in order to obtain necessary services."<sup>67</sup> The Commission found that while the handset market was fully competitive, the cellular service market was not, thus "leaving open the possibility that bundling may be used for anticompetitive purpose."<sup>68</sup> Nevertheless, the Commission concluded that "the public interest benefits of bundling in the cellular market outweigh the potential for competitive harm."<sup>69</sup> In particular, the Commission found benefit in "the provision of discounted CPE to customers who otherwise would not subscribe to cellular service and the promotion of efficient spectrum utilization by adding new customers to cellular service."<sup>70</sup> It lauded handset discounts as a means of expanding cellular service, given that "the high price of CPE represents the greatest barrier to inducing subscription to cellular service."<sup>71</sup> In its ruling, the Commission permitted carriers to offer handsets and services as a bundled package so long as consumers could still obtain service at a nondiscriminatory price without purchasing a handset from the carrier.<sup>72</sup>

Acting at the direction of Congress four years later, the FCC adopted rules to require both that wireline local exchange carriers offer local number portability for customers who wished to move to a mobile carrier, and that mobile carriers offer number portability for customers who wish to switch mobile carriers or move to a wireline telephone

---

66. Bundling of Cellular Customer Premises Equip. & Cellular Serv., *Report & Order*, 7 FCC Rcd. 4028, ¶1 (1992).

67. *Id.* ¶ 6.

68. *Id.*

69. *Id.* ¶ 7.

70. *Id.*

71. *Id.* ¶ 19. The Commission's assessment of public interest received indirect judicial support in antitrust litigation against the five largest wireless carriers, in which plaintiffs argued that each defendant's practice of requiring customers to purchase an approved handset constituted an unlawful tying arrangement. In rejecting plaintiffs' claim, the court noted that "wireless service providers continue to package service and handsets, subsidizing the latter, 'to continue to open markets and make it affordable' for consumers to obtain wireless service." In re Wireless Tel. Servs. Antitrust Litig., 385 F.Supp.2d 403, 410 (S.D.N.Y. 2005).

72. Bundling of Cellular Customer Premises Equip. & Cellular Serv., *supra* note 66, at ¶ 30.

company.<sup>73</sup> In essence, pursuant to the Commission's requirement of "service provider portability," carriers were required to enable "end users to retain the same telephone numbers as they change from one service provider to another."<sup>74</sup> And pursuant to the Commission's requirement of "service portability," carriers were required to enable end users to retain their number when changing from one kind of service to another.<sup>75</sup> The Commission determined that number portability gave consumers greater ability to move from one service provider and kind of service to another, and thus promoted greater competition in telecommunications services. As the Commission stated:

The ability of end users to retain their telephone numbers when changing service providers gives customers flexibility in the quality, price, and variety of telecommunications services they can choose to purchase. Number portability promotes competition between telecommunications services by, among other things, allowing customers to respond to price and service changes without changing their telephone numbers. The resulting competition will benefit all users of telecommunications services.<sup>76</sup>

Under Commission rules, mobile carriers have been required to provide number portability beginning in November 2003.<sup>77</sup> The FCC has found significant wireless number porting since then. Some 20.4 million wireless subscribers ported their numbers to another wireless carrier from December 2003 through December 2005.<sup>78</sup> Nonetheless, the Commission has also found that "the advent of porting in late 2003 did not lead to a significant increase in wireless churn, but did appear to have had a positive impact on service quality by inducing carriers to engage in aggressive customer retention efforts."<sup>79</sup> According to one industry

---

73. Tel. No. Portability, *Second Memorandum Opinion & Order on Reconsideration*, 13 FCC Rcd. 21,204 (1998), available at [http://www.fcc.gov/Bureaus/Common\\_Carrier/Orders/1998/fcc98275.txt](http://www.fcc.gov/Bureaus/Common_Carrier/Orders/1998/fcc98275.txt); Tel. No. Portability, *First Memorandum Opinion & Order on Reconsideration*, 12 FCC Rcd. 7236 (1997), available at [http://www.fcc.gov/Bureaus/Common\\_Carrier/Orders/1997/fcc97074pdf.html](http://www.fcc.gov/Bureaus/Common_Carrier/Orders/1997/fcc97074pdf.html); Tel. No. Portability, *First Report & Order & Further Notice of Proposed Rulemaking*, 11 FCC Rcd. 8352 (1996), available at [http://www.fcc.gov/Bureaus/Common\\_Carrier/Orders/1996/fcc96286.txt](http://www.fcc.gov/Bureaus/Common_Carrier/Orders/1996/fcc96286.txt) [hereinafter *First Portability Order*].

74. *First Portability Order*, *supra* note 73, at ¶ 172.

75. *Id.* ¶ 174.

76. *Id.* ¶ 30.

77. Under the Commission's rules commercial mobile carriers operating the 100 largest Metropolitan Statistical Areas ("MSAs") were required to be providing number portability by November 24, 2003, and those outside the largest MSAs were required to be local number portability-capable by May 24, 2004. FCC 2006 Mobile Services Report, *supra* note 19, at 65.

78. *Id.* at 66.

79. *Id.* at 67.



analyst, such efforts have included “better deals on upgrade handsets, incentives for signing longer contracts, better customer service, and higher network spending.”<sup>80</sup> Certainly, the carriers’ near universal practice of locking handsets is also a factor in curbing subscriber churn.

How then should the FCC view carriers’ use of DRM on content to impose a barrier to subscriber mobility? Should the Commission view it as an undesirable burden on competition, much like the carriers’ now-outlawed requirement that subscribers change their phone number in order to move to a new carrier? Or should the Commission view it as a content-equipment-service bundle that might lead to reduced prices for basic cellular phone service and thus expand availability to low-income consumers? Or rather, should the Commission view carriers’ use of DRM even to lock in subscribers as a necessary impetus to spurring the transformation of mobile carriers from suppliers of cellular phone service to providers of a broad range of mobile data services, with possible pro-competitive impact on music and multi-channel video programming markets in general?

In the background, on some accounts, the cellular phone service industry has become even less competitive than at the time of the Commissions’ 1992 ruling on handset-service bundling. A leading treatise on telecommunications policy, published in 2005, states that competition in that market is “fierce: the overwhelming majority of the population lives in a county served by at least four alternative providers of wireless services.”<sup>81</sup> And the treatise concludes: “[t]here is a broad consensus that this competition has made pervasive regulation of the wireless market unnecessary.”<sup>82</sup> But industry mergers leave a market that is actually highly concentrated, with four national carriers that dominate the industry. Recent studies conclude that by 2005, a series of mobile carrier mergers had raised the national level Herfindahl-Hirschman Index (“HHI”) to 2300 and the mean HHI for local geographical markets for which mobile phone licenses are issued to above 6000.<sup>83</sup> The Department of Justice considers any market with an

---

80. *Id.*

81. JONATHAN E. NUECHTERLEIN & PHILIP J. WEISER, *DIGITAL CROSSROADS: AMERICAN TELECOMMUNICATIONS POLICY IN THE INTERNET AGE* 261 (2005).

82. *Id.* at 262.

83. Jeremy T. Fox & Hector Perez, *Mobile Phone Mergers and Market Shares: Short Term Losses and Long Term Gains* 7 (Networks, Elec. Commerce, and Telecomms. (“NET”) Inst. Working Paper #06-16, 2006), available at <http://www.netinst.org/Fox2006.pdf>; Jeremy T. Fox, *Consolidation in the Wireless Phone Industry* 16 (NET Inst. Working Paper #05-13, 2005), available at <http://www.netinst.org/Fox2005.pdf>. The FCC finds that the average value of HHIs weighted by geographic market population is “only” 2706. But the FCC uses a metric for measuring geographical markets and concentration in those markets that, it admits, tends to “understate systematically the actual level of market concentration.” FCC 2006 Mobile Services Report, *supra* note 19, at 13 n.89.

HHI above 1800 to be “highly concentrated”.<sup>84</sup> The national market is also characterized by high entry barriers and significant economies of scale.<sup>85</sup> Like other telecommunications industries, therefore, the mobile carrier market has built-in tendencies to oligopoly.<sup>86</sup>

Seen in that perspective, FCC rules to ensure that mobile subscribers may freely move from one carrier to another appear warranted to promote competition in the industry. While subscriber churn is not a good in and of itself, we want mobile carriers to aim to keep existing subscribers by providing better service at lower price, not by using DRM to lock them in. There seems to be a consensus, even among consumer advocates, that government regulation is not needed to force interoperability of devices that play content at this point generally.<sup>87</sup> However, there might be reasons to do so in the highly concentrated mobile carrier industry nonetheless. At the very least, the Commission might require adequate advance notice to subscribers that whatever content they download will be lost if they move to another carrier (if that in fact becomes the business model). In that way, consumers will be able, at least in theory, to take switching costs into account in their decisions to purchase content.<sup>88</sup> As former FCC Chairman Powell has aptly put it: “consumers must receive clear and meaningful information regarding their service plans and what the limits of those plans are. Simply put, information is absolutely necessary to ensure that the market is working.”<sup>89</sup>

Yet on the other hand, mobile carriers will very soon find themselves in intense competition with other providers of content and communication. Markets and technology are exerting considerable pressure towards convergence and transportability, a world in which digital content would be seamlessly transportable across platforms within any given media and across different devices and services. In that world, content obtained from any network or source could be accessible through

---

84. U.S. DEP'T OF JUSTICE AND FED. TRADE COMM'N, 1992 HORIZONTAL MERGER GUIDELINES § 1.51(c) (revised in 1997), available at <http://www.ftc.gov/bc/docs/horizmer.shtm>.

85. See FCC 2006 Mobile Services Report, *supra* note 19, at 22, 26-38.

86. Eli M. Noam, *Fundamental Instability: Why Telecom is Becoming a Cyclical and Oligopolistic Industry*, 18 INFO. ECON. & POL'Y 272 (2006).

87. See generally *Digital Music Interoperability and Availability: Hearing Before the Subcomm. on Courts, the Internet, and Intellectual Property of the H. Comm. on the Judiciary*, 109th Cong. 1 (2006).

88. See generally Oren Bar-Gill, *Bundling and Consumer Misperception*, 73 U. CHI. L. REV. 33 (2006); Joseph Farrell & Paul Klemperer, *Coordination and Lock-in: Competition with Switching Costs and Network Effects* (May 2006) (unpublished paper), available at [http://www.nuff.ox.ac.uk/users/klemperer/Farrell\\_KlempererWP.pdf](http://www.nuff.ox.ac.uk/users/klemperer/Farrell_KlempererWP.pdf).

89. Michael K. Powell, *Preserving Internet Freedom: Guiding Principles for the Industry*, 3 J. ON TELECOMM. & HIGH TECH. L. 5, 12 (2004).

any consumer entertainment or communications device (but, depending on the efficacy and market acceptance of DRM controls, perhaps not freely copied or transferred to others). I could watch a TV program on my computer, handheld media player, or any TV monitor within my home network regardless of whether I have originally accessed or copied the program with my digital video recorder, handheld media player, or computer and regardless of whether the program originates from a broadcaster, webcaster, Internet download site, licensed peer-to-peer (or “superdistribution”), or cellular network. With the growth of Wi-Fi enabled mobile phones, moreover, the mobile carriers’ closed communications networks may well face competitive pressure similar to that which will likely overwhelm content distribution and consumption.<sup>90</sup>

In that world of widespread interoperability, competition will focus on which device and service becomes central to consumers. Will it be the mobile carrier multimedia handset and cellular network; handheld Wi-Fi devices capable of Web browsing, Voice-over-IP communication, and receiving music and video webcasting; set-top boxes that can exchange content with other devices on the consumer’s network; or any of several other combinations and possibilities?

In the face of that fierce inter-industry competition, mobile carriers will have every incentive to provide premium content in as user-friendly a means and as low a price as possible. There are already reports that “intense competition, coupled with an appreciation of AOL’s [failed] walled garden ‘experience,’ have compelled the [mobile] operators to reduce the costs of accessing the growing range of mobile content.”<sup>91</sup> Those cost reductions could well be the first step in the dismantling of the carriers’ walled garden models as well.

At the very least, any DRM-backed proprietary platform will have

---

90. See *Martin Defends Draft 700 MHz Band Order as Democrats Express Qualified Support*, TELECOMM. REP. DAILY, July 24, 2007, 2007 WLNR 14155954 (reporting FCC Commissioner Robert McDowell’s statement that with the growth of Wi-Fi enabled mobile phones, the walled garden model of the major mobile phone carriers is already starting to dissolve); see also Jessica E. Vascellaro & Amol Sharma, *Cellphones Get Wi-Fi, Adding Network Options*, WALL ST. J., June 27, 2007, at B1 (reporting on the immediate promise for mobile carriers, but also the ultimate threat to proprietary networks, posed by Wi-Fi enabled mobile phones). The FCC seems poised to make available vast new spectrum for open communications networks (as well as mobile carriers’ proprietary networks), the remaining question being, “how much?” See Kim Hart, *Verizon Changes Course, Supports Open-Access Plan*, WASH. POST, July 26, 2007, at D08. That will accelerate Wi-Fi mobile communications competition.

91. Damian Blackden, *The World: How Emerging Markets Drive Mobile Marketing*, CAMPAIGN, July 20, 2007, 2007 WLNR 13882956. On the failure of the proprietary, walled garden business model of AOL, CompuServe, and other early Internet service providers in the face of consumer desire to find information and engage in communication on the wide-open Internet, see Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 1992-94 (2006).

to provide significant added-value over open networks to remain tenable. To the extent there arises a world of multiple, largely open platforms for communication and content distribution – and whether it arises depends on myriad market, technological, and regulatory developments – a mobile carrier that imposes DRM merely to make it more difficult for subscribers to move to another mobile carrier would quickly find itself surpassed by other platforms, devices, and networks as consumers' first choice for content and communication. Hence, if regulators are concerned about mobile carriers' use of DRM to combat subscriber churn, they might do best to foster the unhindered development and deployment of new, open platforms and to spur greater cross-sectoral interoperability rather than to focus narrowly on a given industry. That way, competition in information platforms will lead to greater availability of content and communications services regardless of some providers' use of DRM to tether content to their particular platform.

#### CONCLUSION

Following the iPhone's lead, mobile carriers have every temptation to use DRM on the music and video they distribute to lock in subscribers and bolster their walled garden communications networks. At present, their use of DRM in that manner, for that purpose, would likely find enforcement support in the DMCA's anti-circumvention provisions and face no regulatory obstacles at the FCC. At the same time, like Apple, the carriers will face competitive and, possibly, regulatory pressures to provide content that is either DRM-free or transportable across a number of platforms and devices. It is too soon to tell whether, as Wi-Fi enabled mobile devices proliferate, the open Internet will overwhelm the carriers' walled garden networks and force entertainment media to acquiesce in DRM-free content distribution. Much depends on regulatory choice, including the extent to which the FCC makes available new spectrum for open network communication. It is apparent, however, that in the long run, regulators' fostering of a multiplicity of platforms for communication and content distribution, coupled with some degree of cross-platform interoperability, will do more to promote the goals of the Copyright and Telecommunications Acts than would regulation that narrowly targets mobile carriers' use of DRM to combat subscriber churn.