VIRGINIA JOURNAL OF LAW & TECHNOLOGY

SUMMER 2012 UNIVERSITY OF VIRGINIA VOL. 17, NO. 02

Digital Rights Management Lite: Freeing Ebooks from Reader Devices and Software

Can Digital Visible Watermarks in ebooks Qualify for Anti-circumvention Protection under the Digital Millennium Copyright Act?

DANA B. ROBINSON †

ABSTRACT

With explosive growth in the ebook market, publishers are looking for ways to effectively distribute ebooks while preventing them from being resold or used in violation of the terms of use. The current market is dominated by ebook-reader software and hardware, which is intended to control the ebook and prevent its redistribution. However, users want ebooks free of constraints and can easily crack the digital rights management (DRM). Those intent on misconduct are not stopped by DRM, while honorable consumers are punished by complicated DRM solutions.

This Article proposes a solution that allows ebooks to be sold as portable documents that can be used without technical restriction. The Article proposes a novel solution that the author calls DRM Lite, consisting of a visible digital watermark containing the consumer's personal information as well as publishing information, as a means of preventing the redistribution of an ebook.

† Adjunct Professor of Law at the University of San Diego School of Law in the field of intellectual property; expertise includes a broad base of intellectual property law. Mr. Robinson is a founding partner of TechLaw, LLP, where his practice focuses on trademarks and copyrights. His practice includes ebooks and digital publishing. Mr. Robinson can be reached at dana@techlawllp.com. Special thanks to law student Kayla Jimenez for her assistance and research. The views expressed herein are solely those of the author and do not necessarily reflect those of the Department of Justice or any component or officer thereof.

TABLE OF CONTENTS

I. INTRODUCTION

The growth of the ebook market is exponential. From 2008 to 2010, the market grew by more than 1000%[1] and by more than 200% from 2010 to 2011.[2] Sales figures show that ebook sales in January-February 2011 increased by 169.4% over sales from January-February 2010, while all categories combined of print trade books declined by 24.8% over the same period.[3]

Publishers face a dilemma: how to increase distribution of ebooks, while preventing those ebooks from being redistributed by the customer. Publishers heretofore have avoided distributing ebooks in pure text documents or in PDF. Instead, publishers have tied their ebooks to software or hardware in an effort to ensure that the ebooks are not freely copied or distributed, resold, or rented.

But the reality of modern technology is that a technical novice can easily untie an ebook from any software or hardware in minutes. Customers are calling for the removal of technical restraints, not so that the consumer can resell the book, but so that the consumer can read the book on any device and not hassle with passwords or other technical hurdles. Thus, in the next few years, publishers will have to find ways to allow their customers to easily purchase and access ebooks without the constraints of software, hardware, or passwords. Pottermore, of the Harry Potter publishing empire, has led the way by not only offering ebooks free of digital rights management (DRM) but also

[1] Cathy Bussewitz, *The E-book Evolution*, PRESS DEMOCRAT (Jan. 8, 2012, 8:25 AM), http://www.pressdemocrat.com/article/20120108/BUSINESS/120109652/1036/news?Title=Local-publishers-retailers-face-e-book-trend&tc=ar; *see also BookStats Publishing Formats Highlights*, ASS'N AM. PUBLISHERS, http://publishers.org/bookstats/formats (last visited May 25, 2012).
[2] Andi Sporkin, *Popularity of Books in Digital Platforms Continues to Grow, According to AAP Publishers February 2011 Sales Report*, ASS'N AM. PUBLISHERS (Apr. 14, 2011), http://www.publishers.org/press/30/.
[3] *Id.*

requiring that Amazon send customers to its own site to purchase non-DRM ebooks and then sending the customer back to Amazon to download the ebook file for the Kindle that does use DRM.[4]

This Article proposes a simple means of providing publishers with assurance that the customer will comply with the terms of use, while at the same time giving the customer an easily accessible portable document without any hassles. The solution is as simple as using a digital watermark on the ebook that displays the personal information of the customer who purchases the ebook, together with publishing information and a clickwrap agreement.

II. BACKGROUND

Copyright owners have spent the past decade trying to determine how to protect their works from piracy and theft in the digital world. A significant move toward providing protection for copyright holders came with the Digital Millennium Copyright Act (DMCA).[5] The DMCA provides a variety of protections for digital works, such as § 1201, which prohibits the "circumvention" of "a technological measure that effectively controls access to a work protected under this title."[6] The DMCA also prohibits the removal of copyright management information (CMI), which includes the work's title, author, and the copyright owner, as well as certain other information.[7] Prior to the DMCA, Congress was devoting significant attention to the problems faced by copyright enforcement in the digital age.[8] This legislative effort resulted in the DMCA, signed into law October 28, 1998.

From the beginning of digital media, rights holders have attempted to protect their works with technological measures known as "digital rights management" or DRM.

DRM is typically software or another technological method used to control access to a work. In the non-ebook space, DRM might employ a username or password, or software that prevents a digital file from being copied. DRM often includes CMI and other traceable information, such as unique serial numbers.[9] The goal of DRM is to

---

[4] Mike Shatzkin, *The Ebook Marketplace is a Long Way from Settled*, THE IDEA LOGICAL COMPANY (May 7, 2012, 7:58 AM), http://www.idealog.com/blog/the-ebook-marketplace-is-a-long-way-from-settled?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+idealog%2Ftllc+%28The+Shatzkin+Files%29.

[5] Digital Millennium Copyright Act, 17 U.S.C. §§ 1201–1205 (2006).

[6] 17 U.S.C. § 1201(a)(1)(A).

[7] 17 U.S.C. § 1202(c).

[8] *See, e.g.*, *WIPO Copyright Treaties Implementation Act and Online Copyright Liability Limitation Act: Hearing on H.R. 2281 and H.R. 2280 Before the Subcomm. on Courts and Intellectual Property of the H. Comm. on the Judiciary*, 105th Cong. (1997); *NII Copyright Protection Act of 1995: Hearings on H.R. 2441 Before the Subcomm. on Courts and Intellectual Property of the H. Comm. on the Judiciary*, 104th Cong. (1996); *NII Copyright Protection Act of 1995: Joint Hearing on H.R. 2441 and S. 1284 Before the Subcomm. on Courts and Intellectual Property of the H. Comm. on the Judiciary and the S. Comm. on the Judiciary*, 104th Cong. (1995); H.R. REP. NO. 105-551 (1998); S. REP. NO. 105-190 (1998).

[9] World Intellectual Prop. Org. [WIPO], *Current Developments in the Field of Digital Rights Management*, SCCR/10/2 Rev. (May 4, 2004).

prevent someone other than the original purchaser from using or copying the work. First efforts at DRM only prohibited the user from copying digital works, but DRM now can control viewing, copying, printing, and altering of any kind of content. This is made possible through software such as "ContentGuard," which allows a copyright holder to set restrictions on content by defining user and usage rights through data encryption.[10] With certain non-ebook DRM, the copyright holder could develop an enforcement model that verifies user identification and track the use of that content so that a buyer could only use the content the way the copyright holder intended when he originally assigned DRM through the software.[11] DRM makes it difficult to copy a software CD, or a video on a DVD. DRM was long used to prevent the copying of songs purchased on iTunes, although Apple has dropped DRM on its iTunes files.[12] DRM is used to prevent use of a Kindle ebook on other devices. It is also used to prevent iPhone and iPad ebooks from being used on other devices or being transferred between devices.

While this describes the landscape of DRM in the context of video, DVD, music, and software, DRM for ebooks is largely handled either through hardware such as the Kindle or Nook, or through software offered by Adobe called Adobe Content Server. Adobe Content Server is used to wrap books created in a format known as epub, a format that is readable by ebook reader devices, as well as ebook software such as iBooks, Aldiko, and Google Books.[13]

One might say that DRM is now ubiquitous; virtually every digital file offered for sale has some form of DRM. However, the circumvention of DRM is not terribly difficult. Simple "cracks," or software scripts that can be used to unsecure the media from the DRM are common.[14] A DRM-enabled ebook can be "cracked" in minutes by a technical novice.[15] Calibre offers a tool for removing an ebook from Adobe's DRM.[16] But consumers complain about DRM as a hassle that they do not want to deal with.[17] In the current state of affairs, those who are intent on getting at the media free of DRM can do so easily, but honest consumers are impaired and maddened by DRM measures that complicate their free use of a legitimate purchase. As a result, the publishing world has been faced with a quagmire: how to make customers happy while looking for ways to

---

[10] *See* CONTENT GUARD, http://www.contentguard.com (last visited May 26, 2012) (noting that the company sold to Pendrell Technologies in 2011 for ninety million dollars).

[11] Julia Layton, *How Digital Rights Management Works*, HOW STUFF WORKS, http://computer.howstuffworks.com/drm2.htm (last visited May 26, 2012).

[12] *See* Brad Stone, *Want to Copy iTunes Music? Go Ahead, Apple Says*, N.Y. TIMES, Jan. 6, 2009, http://www.nytimes.com/2009/01/07/technology/companies/07apple.html.

[13] *See* Aaron, DeMott, *ePub Reader Software*, JEDISABER.COM, http://www.jedisaber.com/eBooks/Readers.shtml (last updated Dec. 5, 2011).

[14] *See* Charlie Sorrel, *How to Strip DRM from Kindle E-Books and Others,* WIRED, (Jan. 17, 2011, 7:06 AM), http://www.wired.com/gadgetlab/2011/01/how-to-strip-drm-from-kindle-e-books-and-others/.

[15] *Id.*

[16] *See* CALIBRE, www.calibre-ebook.com (last visited May 26, 2012).

[17] *See What is DRM? Digital Restrictions Management – We Oppose DRM!*, DEFECTIVE BY DESIGN, http://www.defectivebydesign.org (last visited Apr. 20, 2012).

mitigate a real threat of illegal copying and mass distribution.[18] Given the fact that it is common knowledge that DRM is easily broken and that consumers prefer not to have their purchases hampered by unnecessary technological protections, some ebook publishers are taking the position that they would rather have *no* DRM than have DRM that makes life hard for the customer.[19] Publishers of ebooks want happy customers. That should be priority number one.

There are various justifications for why publishers use DRM, even though they are aware that it is futile against anyone who desires to crack it. The term "piracy" is frequently raised. However, most publishers of ebooks are not going to use DRM as an anti-piracy mechanism.[20] One study even shows a net gain in sales of legitimate books where the book has been pirated.[21] Beyond piracy, what are the real concerns? The publisher should not terribly be worried that the customer will give this book to his son or wife when he is done reading it. Family members have probably always shared printed books, rather than buying multiple copies. The publisher does not need DRM to prevent minor infractions, as most publishers should not care about sharing ebooks between family and close friends, and some ebook publishers even permit it.[22] The publisher is willing to accept that its ebooks will be shared to some extent with a few other people in the customer's friends and family network. Printed books were generally shared in a similar way. Kindle allows ebooks to be shared among households, and even loaned to third parties. [23] Given that publishers cannot use DRM for anti-piracy and that pursuing their customers for minor infractions is a futile effort, one might say that ebook publishers appear willing to forego DRM altogether.[24]

In fact, the survival of the publishing industry may hinge on the ability of publishers to sell ebooks without being tied to readers like the Kindle. One commentator argues that the publishing industry is becoming a "walled garden" by virtue of the power that Amazon and Apple have over the publishers.[25] Publishers have given this power to

---

[18] *See The Pros, Cons, and Future of DRM*, CBC NEWS (Aug. 7, 2009, 4:12 PM), http://www.cbc.ca/news/technology/story/2009/08/06/tech-digital-locks-drm-tpm-rights-management-protection-measures-copyright-copy-protection.html.

[19] Jenn Webb, *Book Piracy: Less DRM, More Data*, O'REILLY RADAR (Jan. 10, 2011), http://radar.oreilly.com/2011/01/book-piracy-drm-data.html; *see also* Jeremy Greenfield, *Bookseller Backed by Big Publishers Advocates Abandoning Digital Rights Management*, DIGITAL BOOK WORLD (Jan. 25, 2012), http://www.digitalbookworld.com/2012/bookseller-backed-by-big-publishers-advocates-abandoning-digital-rights-management/.

[20] Certainly publishers will enforce against piracy and seek government intervention for criminal enforcement. However, the DRM used by publishers is not intended to target such behavior.

[21] Webb, *supra* note 19.

[22] *See Lending Kindle Books*, AMAZON.COM, http://www.amazon.com/gp/help/customer/display.html/ref=hp_200386160_loan?ie=UTF8&nodeId=200549320 (last visited Apr. 20, 2012) (describing Amazon's Kindle loan policy, which allows certain books to be loaned by another user for fourteen days).

[23] *Id.*

[24] Shatzkin, *supra* note 4 (noting Pottermore's defection to DRM-free distribution and Macmillan's segment tor.com, going DRM-free).

[25] Mathew Ingram, *How the E-book Landscape Is Becoming a Walled Garden*, GIGAOM (Feb. 29, 2012, 2:58 PM), http://gigaom.com/2012/02/29/how-the-e-book-landscape-is-becoming-a-walled-garden/.

Amazon and Apple out of fear of distributing ebooks without DRM.[26] Publishers, in their desire to prevent copying and piracy, unwittingly handed their futures to Amazon (which has an incentive to sell cheap to get more customers who then buy other high-profit Amazon products) and Apple (which has an incentive to sell more devices). The motivation of these large companies is not to help the publishing industry flourish but to serve their own ends. If publishers are going to break free from the control that Amazon and Apple have over the industry, they will have to find a way to either distribute ebooks without DRM or distribute ebooks with a type of DRM that allows users to use ebooks across multiple platforms or on no platform at all.

Publishers are not ready to go DRM-free. Thus, a new question has begun to percolate in the publishing world: What is the minimum necessary DRM that will be accepted by the original publisher?

III. THE MINIMALIST APPROACH TO DRM: IT'S NOT ABOUT PREVENTING COPYING OR ACCESS, BUT ABOUT PRESERVING THE RIGHT TO ENFORCE UNDER THE DMCA.

In order to answer the question of what the minimum necessary DRM is required by the original publisher, we must ask *why* the original publisher requires digital rights management in the first place.

There are a plethora of papers and articles discussing the problem of piracy of digital media and the need for digital rights management that enables users to have free use of their legitimate purchase but still prevents piracy.[27] But what if the problem is not piracy? In the context of ebooks, a pirate need only go buy a book off the shelf and scan and distribute it. As already noted, an unsophisticated person can use readily available software to "crack" an ebook, and easily distribute it. Anyone intent on piracy can do so easily. No amount of DRM will prevent piracy in the context of ebooks. Piracy can be fought on a different front, for example, by use of serial numbers and copyright management information ("CMI") to track and prevent piracy as it relates to outright counterfeits. For purposes of this Article, I believe that piracy is not the core issue to the DRM discussion and that DRM is an ineffective barrier to piracy of ebooks. Those who want to violate copyright law by mass distribution of counterfeit ebooks will not be hampered by DRM.

Therefore, I will assume that the publisher should not be concerned—at least in the case of ebook DRM—with piracy. Publishers should be focusing less on anti-copying and anti-piracy in the context of ebook distribution and focusing instead on how to prevent something more likely, and more injurious to the ebook market: *aftermarkets*. From a business perspective, ebook publishers would like DRM that minimally satisfies

---

[26] *Id.*; *see also* Mark Henricks, *Amazon: The Elephant in the Room*, BOOK BUS. MAG., March/April 2012, at 14.

[27] *See* Bruce Schneier, *Quickest Patch Ever*, WIRED (Sept. 7, 2006), http://www.wired.com/politics/security/commentary/securitymatters/2006/09/71738; Tekla S. Perry, *Loser: DVD Copy Protection, Take 2*, IEEE SPECTRUM (Jan. 2005), http://spectrum.ieee.org/consumer-electronics/standards/loser-dvd-copy-protection-take-2; Michael Arrington, *Bill Gates on the Future of DRM*, TECHCRUNCH (Dec. 14, 2006), http://techcrunch.com/2006/12/14/bill-gates-on-the-future-of-drm.

the DMCA to protect themselves against secondary markets for ebooks that arise after an ebook has been legitimately purchased. However, they do not want to frustrate customers with cumbersome DRM. In other words, publishers may not actually care about the efficacy of the DRM as much as whether the DRM qualifies for protection under the DMCA such that the publisher can prevent books from being sold in aftermarkets.

Aftermarkets are the markets in which an ebook might be sold after it has been purchased by the first retail customer. The most significant aftermarket is the resale market, or "used ebook" market.[28] Traditional aftermarkets for physical goods (such as used printed books or used CD stores) operate under the auspices of the "first-sale" doctrine, which permits the purchaser of a copyrighted work to dispose of it without any say-so from the copyright owner. The brick and mortar "used bookstore" is an example of the classic aftermarket for used printed books. In the context of non-digital media, many websites exist to facilitate the sale of used books, CDs and movies, such as Alibris.com, Amazon.com, eBay, and AbeBooks.com.

The non-digital printed book "used" market is a perfectly acceptable form of aftermarket under the first-sale doctrine.[29] However, as media sheds its physical attributes, a new problem arises. The problem is that ebooks are not physical, and thus, every resale of a so-called "used" *ebook* erodes the ability of the publisher to sell its ebooks. Even though print books are sold in used bookstores, publishers of digital books want to prevent this type of conduct because ebooks are unlike printed books. Printed books cannot be emailed. Printed books degrade over time, while ebooks will maintain their quality.

The U.S. Copyright Office has refused to apply a doctrine of "first sale" to ebooks.[30] The approach taken by the Copyright Office appears to be parallel with the approach taken for computer software.[31] The first-sale doctrine does not apply to computer software.[32] While not the primary subject of this Article, the Copyright Office analysis in the Executive Summary for the DMCA is an excellent overview of first sale in the context of digital media.[33] The Copyright Office refused to endorse the adoption of a "digital first-sale doctrine." As a result, at least one author has concluded that in order to resell digital downloads, consumers will have to also sell their hard drive, ebook reader, or iPod.[34]

---

[28] Aftermarkets also include rental, sharing, trading, and similar markets for "used" media.
[29] 17 U.S.C. § 109(a) (2012).
[30] *DMCA Report Executive Summary*, U.S. COPYRIGHT OFFICE, http://www.copyright.gov/reports/studies/dmca/dmca_executive.html (last visited May 28, 2012).
[31] *See* 17 U.S.C. § 117 (2012).
[32] *See* 17 U.S.C. § 109(b)(1)(A), 109(d) (2012) (stating that under the plain language of the Copyright Act, a license is not subject to the first sale doctrine or § 117); *see also* Apple Inc. v. Psystar Corp., 658 F.3d 1150, 1155 (9th Cir. 2011) ("[T]he [copyright] statute specifically excludes the doctrine's application, however, when the copy is transferred through 'rental, lease, loan, or otherwise, without acquiring ownership of it.' Thus, the first sale doctrine does not apply to a licensee.").
[33] *DMCA Report Executive Summary*, *supra* note 30.
[34] Seth Greenstein, *Would You Sell Your Kindle to Sell a Used Book*?, CNN MONEY (Dec. 23, 2010, 12:18 PM), http://tech.fortune.cnn.com/2010/12/23/what-do-you-really-own-when-you-buy-an-e-book.

It is unlikely that people will sell their devices as a means of selling their ebooks. Devices are quite expensive. It seems unlikely that a used market will arise for tablet devices based on the content downloaded to the device. But digital books are portable. They can be copied. A person can copy her ebook, retain a copy, and email the other copy to someone else. While this is likely illegal under the current state of the law, publishers want to prevent this from impacting their market without having to sue the individual consumer. In this regard, publishers should be worried about secondary markets, such as used ebook stores, resale of ebooks on auction sites like eBay, and ebook rental markets. If a consumer can rent an ebook from a website for $1.00, why would they buy the ebook for $10.00? Thus, stakeholders in the ebook industry are looking for ways of preventing "used" ebookstores and rental markets for ebooks.

Some websites have already attempted to enter the market to create sharing and lending platforms. For example, eBookLendingLibrary.com was set to offer lending in early 2011, but ironically, as of the writing of this Article, the site is no longer operating. Swap and lending markets are flourishing for ebooks but are based on legitimate lending permitted by Amazon's Kindle and Barnes & Noble's Nook, such as ebookfling.com and Booklending.com. However, there do not appear to be any legitimate markets for *used* ebooks. Publishers should fear this market most, and therefore the publishers should desire to ensure that ebooks contain whatever minimal DRM is required to prevent this market from flourishing.

Secondary markets for ebooks present a real threat to ebook publishers. Certainly, publishers would like to prevent consumers from redistributing ebooks. But they may not need to be as concerned about the impact of this on their market. Apple has dropped DRM on iTunes without significant impact on the sale of music. If the price is right, consumers will pay for ebooks. Thus, they should desire to use DRM with a view toward dissuading redistribution, but more importantly as a means of satisfying the DMCA's requirement that a technological measure be circumvented in order to enforce against would-be ebook resale stores.

There are a several methods that an ebook publisher can use to keep its books out of the resale markets. The primary method used to date is simple: ebooks are offered within a contained hardware and software system (a "reader") that makes it very difficult to use the file outside of the device. For iPad books, one must use the ebook on the user's iPad. Barnes & Noble uses the Nook; Amazon offers the Kindle. Kobo entered this market, created a reader device, and sold to a Japanese company named Rakuten for $315 million.[35] Kindle and Nook devices can even facilitate the sharing of ebooks because they can be sure that the original owner of the ebook no longer has access to the book once she loans the ebook. Readers currently define the market for ebooks because ebook reader devices are perceived to offer an optimal DRM solution. However, the reality is that books downloaded to an ebook reader can be "cracked" as easily as any other DRM.[36] As

[35] *Kobo Positioned for International Growth as Acquisition by Rakuten Closes*, CNW GROUP (Jan. 11, 2012, 4:08 PM), http://www.newswire.ca/en/story/904313/kobo-positioned-for-international-growth-as-acquisition-by-rakuten-closes.

[36] *See* Jeremy Kirk, *Hackers Claim Victory in Cracking Amazon Kindle DRM*, PCWORLD (Dec. 23, 2009, 1:20 PM), http://www.pcworld.com/article/185408/hackers_claim_victory_in_cracking_amazon_

for the legalities of consumers' compliance with the DMCA, one commentator has noted ways that ebooks can be cracked without violating the DMCA.[37]

While reader device use is growing rapidly, the future of computing is unlikely to rely on ebook reading devices.[38] Even now, the Kindle is evolving from an ebook-only device to an all-purpose tablet.[39] Tablets are nothing more than computers that the user can hold more easily and interface with the touch of the user's fingers. Thus, as tablets come to the forefront, ebook publishers are "securing" their ebooks with DRM that is part of ebook software (such as Adobe Content Server), rather than a reader *device*. For some period of time, ebooks will be largely distributed through DRM-enabled reader software that works on any computer.

But what if a publisher desired to distribute ebooks that were not tied to reader software? Publishers will have to do this in the near future, or consumers will take it upon themselves to free their ebooks from their devices and software without the publisher's permission. What legal mechanisms could be used to achieve the publisher's goal of selling an ebook without an ebook reader, yet include the minimal DRM necessary to obtain remedies under the DMCA to prevent aftermarkets?

IV. THE SOLUTION

The solution proposed in this Article is to create ebooks in a variety of formats[40] with a visible watermark on each page (or at the end of each chapter). The watermark would contain the personal information of the customer who purchased the ebook and a warning not to resell or distribute the book in any way. The user who purchases such a book will agree to terms and conditions that prohibit copying and distribution, as well as a statement that the consumer's personal information will be prominently displayed on the book as a deterrent from distributing or copying in violation of the agreement. Might this simple approach to "DRM" qualify as a technological protection measure for purposes of the DMCA?

In support of this position, I evaluate a combination of three complimentary techniques to protect ebooks from secondary markets and free them from cumbersome DRM. The proposal calls for the use of a watermark on the pages of the ebook that contains the personal information of the customer, as well as copyright management

---

kindle_drm.html (discussing cracking the Kindle DRM); *see also How Can I Remove iBooks DRM Protection Easily?*, EBOOK DRM REMOVAL, http://www.ebookdrmremoval.com/how-to/remove-ibooks-drm.html (last visited Apr. 20, 2012) (providing steps for cracking the Apple DRM).

[37] *See* Ryan Iwahashi, *How to Circumvent Technological Measures Without Violating The DMCA: An Examination of Technological Protection Measures Under Current Legal Standards*, 26 BERKELEY TECH. L.J. 491, 512–17, 518, 521–22 (2011).

[38] Kristen Purcell, *E-reader Ownership Doubles in Six Months: Tablet Adoption Grows More Slowly*, PEW RESEARCH CENTER (June 27, 2011), http://pewresearch.org/pubs/2039/e-reader-ownership-doubles-tablet-adoption-grows-more-slowly.

[39] *See* Matt Alexander, *The E-Reader, as We Know It, Is Doomed*, THE LOOP (Jan. 4, 2012, 12:02 PM), http://www.loopinsight.com/2012/01/04/the-e-reader-as-we-know-it-is-doomed.

[40] E.g., epub format, mobi format, or portable document format ("PDF").

information, and a clickwrap agreement. Used together, I propose a solution that I call DRM Lite,[41] a solution that should qualify for protection under the DMCA.

A. Terms and Conditions

The sale of ebooks on the Internet can be completed pursuant to an agreement that the user "clicks" when making a purchase. These "clickwrap" agreements are common for other media purchases, and can be used to set forth terms and conditions of use as between the purchaser and the publisher.

Rights holders' first line of defense against improper use of an ebook is through contract law. This is relatively straightforward. Upon the sale of a digital product, an agreement is consummated when the consumer either opens the wrapper (shrinkwrap agreement) or when the user downloads the file online (clickwrap agreement). The rights holder can use contract law in the terms and conditions of use in order prohibit certain conduct. A contract tied to an ebook sale might include some of the following terms:

- You agree not to make copies of this ebook.
- You agree not to resell this ebook.
- You agree not to rent this ebook.
- You agree not to loan this ebook.
- You agree not to distribute copies of this book.
- You agree that this ebook will only be used by you on up to one (1) device at a time, and that you will delete this ebook from a device if you move the ebook to a different device, except that you may keep one (1) backup copy on a secondary digital media storage device, but not as an accessible or usable ebook.
- You agree not to remove the copyright management information contained on this ebook.

Provided the "contract" used to set forth the terms and conditions of purchase and use by the consumer, the rights of the rights holders can be secured by way of agreement, at least between the consumer and the rights holders.[42]

Further, it would seem that a rights holder could present the consumer with an additional requirement that is part of the proposed DRM Lite solution. The rights holder could state in its clickwrap agreement that the ebook will be permanently imprinted with a visible watermark that shows the consumer's name, telephone number, and email

[41] A phrase coined in my discussions with eChristian, Inc. president Cory Verner (an ebook publisher) to whom I am indebted for several points of collaboration and discussion.

[42] *See generally* Cairo, Inc. v. CrossMedia Servs., Inc., No. C 04-04825 JW, 2005 WL 756610, at *5 (N.D. Cal. Apr. 1, 2005); DeJohn v. The .TV Corp. Int'l, 245 F. Supp. 2d 913, 919 (C.D. Ill. 2003); Caspi v. Microsoft Network, L.L.C., 732 A.2d 528, 532 (N.J. Super. Ct. App. Div. 1999); Groff v. Am. Online, Inc., No. PC 97-0331, 1998 WL 307001, at *5 (R.I. Super. Ct. May 27, 1998).

address, as well as a statement that the book belongs to the consumer and any use or access by a third-party is strictly forbidden. Such a clause might look like this:

- You agree that by purchasing this ebook, your personal information will be permanently marked on the pages of the ebook and you agree not to remove or obscure this information.

While some might jump to the conclusion that this is a violation of "privacy,"[43] they must remember that this is an ebook that is being purchased with a consumer being told that this is how the rights will be protected. There has been full disclosure, and she has given permission to embed this information. The consumer's personal information will be embedded at the point of sale, and as long as the owner of that ebook does not violate the agreement, she will never have to worry about privacy concerns. It is her book with her personal information in it. No one else should be viewing this book, and thus, there is no issue of the user's privacy other than the *user* doing something that discloses that personal information, which she may choose to do.

One might call this a form of "moral" DRM. The ebook publisher is asking people to be honest and honor the terms of their agreement to not distribute, loan, rent, or resell the ebook. In exchange, the customer receives an ebook that is not burdened by complicated DRM, and is free of any reader software or device. The consumer can move the ebook between devices and computers easily. The trade-off for this convenience is that the consumer's personal information will be indelibly watermarked on the ebook, holding the consumer accountable to stay true to the terms of the agreement.

Once this personal information ("PI") is embedded on the book, the user would have a significant incentive to NOT violate the other terms of use. A consumer whose name, email and phone number is visible on each page of an ebook will be far less likely to consider reselling, renting, or even sharing the book. The consumer would have no qualms about sharing the book with family and friends. But as noted above, the publishing industry should expect some sharing of content among friends and family.

Thus, with a simple change to the terms of the clickwrap agreement, and the addition of a watermark to the ebook, the publisher will be able to drop the use of cumbersome DRM technology, obtain an agreement not to do certain things, and provide a significant incentive for the consumer to honor the agreement. In practice, this is more likely to prevent ebook misuse than the more technical measures being taken in most other DRM software.

A consumer may still decide to sell the ebook to a "used ebook store." If the book is purchased by a used ebook store, the clickwrap agreement is not binding on that party. Thus, under contract law, the publisher cannot sue the used ebook store. The third-party does not have a contractual obligation with the publisher; there is no privity of contract between the publisher and the third-party. In this case, suing the consumer is undesirable and impractical.

[43] *See* Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 598 (2003).

The publisher must then take a further step in order to have a remedy against the used ebook store rather than the consumer. The used ebook store is not liable for violation of the clickwrap agreement. But the used ebook store is likely to do something that may be actionable. The used ebook store is likely to remove or obscure the watermark. A consumer would not be likely to sell to the used ebook reseller unless the ebook seller had a way of obscuring or removing the watermark. Thus, the consumer would probably only sell its ebook to an ebook reseller who was able to remove or obscure the watermark. In this case, the publisher can seek remedies against the bookstore for removing or obscuring the watermark. Again, while the consumer is cheating, the publisher would probably like to avoid suing its customer. Instead, it wants a way to stop the used ebook seller. It may be able to do so, under one of two provisions of the DMCA.

B. CMI

The DMCA prohibits the removal or falsification of copyright management information, and the distribution of any works wherein such information is removed or falsified.[44] CMI includes the author, rights holder, terms and conditions, identification number(s), and a few other categories of information. Section 1202 is intended to prevent the wide distribution of copyrighted works that fail to include attribution, as well as terms and conditions of use and tracking data such as serial numbers that enable rights holders to track and enforce their rights against piracy and mass distribution by counterfeiters.

The DMCA prohibits the removal of copyright management information by anyone. Thus, the publisher can enforce against a third-party with whom it has no privity of contract. Section 1202 reads as follows:

> (a) False Copyright Management Information.
>
> — No person shall knowingly and with the intent to induce, enable, facilitate, or conceal infringement--
>
> (1) provide copyright management information that is false, or
>
> (2) distribute or import for distribution copyright management information that is false.
>
> (b) Removal or Alteration of Copyright Management Information.
>
> — No person shall, without the authority of the copyright owner or the law--
>
> (1) intentionally remove or alter any copyright management information,
>
> (2) distribute or import for distribution copyright management information knowing that the copyright management information has been removed or altered without authority of the copyright owner or the law, or
>
> (3) distribute, import for distribution, or publicly perform works, copies of works, or phonorecords, knowing that copyright management information has been removed or altered without authority of the copyright owner or

[44] 17 U.S.C. § 1202 (2006).

> the law, knowing, or, with respect to civil remedies under section 1203, having reasonable grounds to know, that it will induce, enable, facilitate, or conceal an infringement of any right under this title.[45]

CMI includes the following information:

> (1) The title and other information identifying the work, including the information set forth on a notice of copyright.
>
> (2) The name of, and other identifying information about, the author of a work.
>
> (3) The name of, and other identifying information about, the copyright owner of the work, including the information set forth in a notice of copyright.
>
> (4) With the exception of public performances of works by radio and television broadcast stations, the name of, and other identifying information about, a performer whose performance is fixed in a work other than an audiovisual work.
>
> (5) With the exception of public performances of works by radio and television broadcast stations, in the case of an audiovisual work, the name of, and other identifying information about, a writer, performer, or director who is credited in the audiovisual work.
>
> (6) Terms and conditions for use of the work.
>
> (7) Identifying numbers or symbols referring to such information or links to such information.
>
> (8) Such other information as the Register of Copyrights may prescribe by regulation, except that the Register of Copyrights may not require the provision of any information concerning the user of a copyrighted work.[46]

CMI does not include "any personally identifying information about a *user* of a work or of a copy, phonorecord, performance, or display of a work."[47]

Removal of CMI is a violation of the DMCA. Removal of CMI is not "circumvention," as that term is used in § 1201, but a separate violation of § 1202's prohibition on removing CMI.

CMI can be embedded in a watermark (visible or not). As professor Nimmer states:

> The legislative history for Section 512's discussion of red flags contains a stray reference to a matter that raises its own puzzles: watermarks. The passage in question refers to "the absence of customary indicia of ownership or authorization, such as a standard and accepted digital watermark or *other* copyright management information." That statement tacitly assumes that a watermark qualifies as CMI. It remains to evaluate that assumption.[48]

---

[45] *Id.*
[46] 17 U.S.C. § 1202(c).
[47] *Id.* (emphasis added).
[48] DAVID NIMMER, COPYRIGHT: SACRED TEXT, TECHNOLOGY, AND THE DMCA 375 (2003).

In our hypothetical scenario, the third-party used ebook reseller wants to remove the *user's* personal information, which can be removed without violating § 1202, as long as it leaves the CMI (i.e., the copyright notice, author's information, serial number, etc.). As such, the wily aftermarketer will avoid violation of § 1202 by leaving that information and carefully removing or obscuring the personal information only.

Thus, the use of contract law plus CMI gets the publisher part of the way, but not all of the way. In order to violate the DMCA under § 1202, the aftermarketer must remove CMI. We want to find a legal mechanism for preventing the used ebook store from removing the personal information of the original customer.

C. Watermark of PI as DRM/DMCA Anti-circumvention Measure

My proposal, though not yet tested, is to identify the watermark of the *user's* "personal information" as a "technological measure" that is intended to control access to a work pursuant to § 1201. If this watermark is considered a "technological measure" under § 1201, then removal of the personal information will constitute a violation of the DMCA and provide a means of enforcement against the used ebook store.

1. The DMCA

The DMCA forbids any person from "circumvent[ing] a technological measure that effectively controls access to a work protected under this title."[49] To "circumvent a technological measure" is "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."[50]

Congress enacted the Digital Millennium Copyright Act ("DMCA") in 1998 to "strengthen copyright protection in the digital age"[51] and to implement the World Intellectual Property Organization Copyright Treaty ("WIPO Treaty"), which requires contracting parties to:

> provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.[52]

Subsection 1201(a)(1)(A) is the anti-circumvention provision, which prohibits a person from "circumvent[ing] a technological measure that effectively controls access to a work protected under [Title 17, governing copyright]," stating: "No person shall

[49] 17 U.S.C. § 1201(a)(1)(A).
[50] *Id.* § 1201(a)(3)(A).
[51] *See* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 435 (2d Cir. 2001).
[52] WIPO Treaty, art. 11, Dec. 20, 1996, S. TREATY DOC. No. 105-17 (1997).

circumvent a technological measure that effectively controls access to a work protected under this title."[53]

As used in this subsection, to "circumvent a technological measure" means "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."[54] In other words, the statute requires something technical that controls access. In the most rudimentary sense, a software application that requires a username and/or password would probably be a "technological measure" and "effectively control access." The question is whether my proposed solution is "technical" enough in the manner in which it controls access.

Again, I propose that ebook publishers watermark the pages of an ebook with the personal information of the consumer who purchases the book. This watermark would be visible and difficult to remove.[55] The watermark could be placed randomly throughout the document. The idea is that by placing the name, email, and/or telephone number of the consumer directly on the pages of the ebook, the consumer would have a motivation *not* to resell the book. This is "technical" and *because of* the content of the watermark, it would "effectively control access" by deputizing the user to not give access to the work for fear of handing out an ebook that has his or her personal information visibly present throughout the ebook.

The focus of this analysis is whether a visible watermark containing personal information of the consumer on an ebook can constitute a type of DRM that will qualify for protection under the anti-circumvention provisions of the DMCA. Is this watermark a technical measure? Would removal (or obscuring) of the watermark constitute a *circumvention* of a *technical measure* intended to control access to a work?

2. DRM "Lite"

I call the proposed watermarking solution "DRM Lite." By "lite" I do not mean low calorie, but a digital rights management scheme that is the minimal required technology to provide a barrier to improper use of a digital work and still qualify for enforcement under the DMCA.

Traditional wisdom is that watermarks are not sufficient to be considered an anti-circumvention technology. As set forth in the statute, "a technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."[56]

---

[53] 17 U.S.C. § 1201(a)(1)(A).
[54] *Id.* § 1201(a)(3); *see also* I.M.S. Inquiry Mgmt. Syss., Ltd. v. Berkshire Info. Syss., Inc., 307 F. Supp. 2d 521, 532–33 (S.D.N.Y. 2004).
[55] Removal would likely have to be done by watermarking a new color over each watermark, or writing a program that could do this automatically. However, such a program would be difficult because it would have to find the placement of the watermark throughout the ebook.
[56] 17 U.S.C. § 1201(a)(3)(B).

In the past, watermarks have been considered passive.[57] Little attention has been given to the idea that a watermark could be something that allows or disallows one from gaining "access" to the work. An example may be found in the *Agfa Monotype* case, where the court held Adobe did not violate DMCA when it used Monotype's fonts, which were embedded with watermarks.[58] The watermarks at issue in *Agfa Monotype* were not intended to prevent copying; and in fact the widespread use of the fonts was encouraged by Agfa Monotype. *Agfa Monotype* illustrated that when a user modifies a program which is embedded with watermarks, the user is not necessarily "circumventing" or violating DCMA 17 U.S.C. § 1201(a)(2)(A) if those "embedded bits" do not control access to the work but merely serve as a "passive" watermark.[59] In *Agfa Monotype*, there was no evidence that the watermarks were used for security or to prevent copying.[60]

However, one can revisit this question in light of the fact that the *content* of the DRM Lite watermark is something that will act to control the conduct of the consumer who owns the ebook. In *Agfa Monotype*, the court found that the watermark was not intended to control access to the work. In my proposed DRM Lite solution, the *content* of the watermark is a feature that is intended to ensure that the *owner* of the work only allows access to those with whom her is willing to share her name, phone number and email address, together with a statement that this named person is a lawbreaker if they permit another to possess this particular ebook. Thus, while the technology alone may not prevent or allow access, the technology of creating an indelible watermark of the user's information at the point of sale, in combination with the PI itself, should constitute a means of controlling access. We are making the user the gatekeeper. The user is deputized by the watermark, incentivized to "prevent access" to the work by virtue of the contents of the watermark. After all, the main point the court made in *Agfa Monotype* was that the "embedded bits" [watermark] did not serve any function of controlling user access to the program. The watermark here does serve to control access.

Courts and academics have concluded that technological measures that "control access to a work" must have some gatekeeping function.[61] Earlier cases indicated that such gatekeeping technologies must ask for a username and/or password, or somehow prevent "access" by anyone other than the rights holder.[62]

---

[57] *See* Agfa Monotype Corp. v. Adobe Sys., Inc., 404 F. Supp. 2d 1030, 1036 (N.D. Ill. 2005).
[58] *Id.*
[59] *Id.*
[60] *Id.* at 1040.
[61] *See* 1 RAYMOND NIMMER, INFORMATION LAW § 4:29 (2d ed. 2002); *see also* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 528 (6th Cir. 2004); Auto Inspection Servs., Inc. v. Flint Auto Auction, Inc., No. 06-15100, 2006 U.S. Dist. LEXIS 87366, at *23 (E.D. Mich. Dec. 4, 2006) ("[T]he user detection feature would not prevent anyone from gaining access to the source code and copying it verbatim" and therefore does not control access to a work as stated in the DCMA); *Agfa*, 404 F. Supp. 2d at 1036 (N.D. Ill. 2005) ("Embedding bits, which are not secret and require no password or authorization, are the only alleged 'technological measure,' and there is nothing to work in conjunction with the embedding bits to control access.").
[62] I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 532 (S.D.N.Y. 2004); *see also* Egilman v. Keller & Heckman, LLP, 401 F. Supp. 2d 105, 113-14 (D.D.C. 2005) (following *I.M.S. Inquiry Mgmt.* and finding that where a party used the actual username/password obtained from dubious sources (it seems from the case that it came from the plaintiff), the use of the actual username/password

However, this view has begun to broaden.[63] In *Lexmark*, for example, while the court did not find that Lexmark's chip was a technological measure that prevented access, it did not find that there was a need for a username or password in order to be considered such.[64] The recent cases seem to support a position that a password is not necessarily required in order for a technological measure to effectively control access.[65] Professor Nimmer has argued that technology which is readily accessible without circumvention may still be legally identical to the work or use under DRM protection by an access control device; he states that even under the *Lexmark* analysis, leaving one door open does not vitiate the DMCA claim.[66]

Perhaps an easy solution to providing DRM that clearly qualifies for DMCA protection would be to require users to access their ebooks via username and password.[67] However, this simple solution may not work in practice. Based on the current state of the law it seems clear that inclusion of username/password would be a "technological measure" under the DMCA. Even so, the use of the username/password by a third-party would not necessarily be a "circumvention" because if a third-party uses the *correct* username/password it is not a circumvention.[68] Thus, the inclusion of a username/password, while qualifying as a technological measure, is not actually helpful to a publisher. By adding a username/password gatekeeper, the publisher burdens the customer while not providing any remedies against an aftermarket unless the aftermarket removes the whole gatekeeper. Why should the publisher use this mechanism when it would not actually prevent the user from distributing the book to secondary markets? All the customer would need to do in order to rent or resell the ebook is share a generic username and password with the purchaser, and both the aftermarket and the purchaser would be free of DMCA liability. This would be DRM without teeth. The customer would be hampered by a bothersome gatekeeper every time he wanted to change devices (entering a username and/or password), and in the end, the customer who wants to rent or resell his ebook can do so without DMCA liability to himself or the reseller. If the original consumer can just pass along credentials and free the next user(s) from liability, then this method, while qualifying for DMCA protection, offers no value to the rights holder because there would be no circumvention.

---

was not enough to be considered a "circumvention," even though the use of the username/password was without authorization); *see also*, Iwahashi, *supra* note 37 at 523 (categorizing watermarking as "very likely no violation" but not addressing watermarking as presented in this Article).

[63] *See* Davidson & Assocs. v. Jung, 422 F.3d 630, 641 (8th Cir. 2005) (expanding "control access to a work" to mean not freely available, as in this case where the online capability of a program was not available freely and was only unlocked to users who purchased the program; therefore, circumventing this access violated the DMCA).

[64] Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 549–50 (6th Cir. 2004).

[65] *See also* MDY Indus., LLC v. Blizzard Entm't, Inc., 63 F.3d 928, 954 (9th Cir. 2010) (where a process was employed to give the user access to the work, and thus circumventing this process/gate-keeping function was a violation of the DCMA).

[66] Nimmer, *supra* note 61.

[67] As a practical matter, if a username/password system were embedded, the ebook would not function on various reader software and devices, such as Kindle and Nook. The goal of the ebook publisher is to use DRM Lite in order to make an ebook portable, readable on every device, or just on a computer or tablet. In trying to surmount this barrier, the solution loses its "lite"-ness.

[68] Egilman v. Keller & Heckman, LLP, 401 F. Supp. 2d 105, 112–13 (D.D.C. 2005).

Moreover, using a solution that requires a username/password is impractical because it would not be compatible across various reader software and devices. If the goal is to provide a consumer with easy-to-use ebooks, they must be free of obstacles such as usernames/passwords, or other technologies that defeat compatibility.

DRM Lite, on the other hand, would not be so easy to bypass without "circumvention." The watermark would need to be removed or obscured to avoid displaying the personal information of the consumer. Assuming DRM Lite is found to be a technological measure, then the removal or obscuring[69] of the watermark would be a circumvention. This would make the removal or obscuring of the DRM Lite watermark a violation of the DMCA, actionable against used ebook stores or third-parties. The publisher gets a more effective DRM because the consumer is unlikely to distribute the ebook with her personal information, and at the same time, the publisher secures its goal of preventing used ebook markets that might remove or obscure the watermark.

3. DRM Lite Plus

While the DRM Lite approach provides a simple and elegant solution to providing an effective DRM tool amenable to DMCA remedies, there is one additional strategy that I would like to suggest. In the revision process of this Article, I provided a draft to Cory Verner.[70] He suggested something that takes DRM Lite to a new level. An ebook publisher could embed CMI within the PI watermark. For example, if a serial number were to be embedded (visibly or invisibly) into the PI, if someone removed or obscured the PI watermark, they would also be removing CMI. The removal of CMI is actionable under § 1202. Thus, even if a court found that removal of the PI watermark was not a violation of § 1201, the party would be guilty of removing CMI under § 1202. Imagine a watermark that shows the consumer's name and email address at random places, but in tiny print inside the font of the watermark there is a serial number, qualifying that information for CMI and making its removal a violation of § 1202. That solution would seem to offer the publisher more practical protection than any complicated DRM software on the market, while giving the consumer a smooth experience.

V. CONCLUSION

Given the rapid growth of the ebook market and the ease with which DRM can be cracked, publishers must look for ways to give their customer an easy-to-use ebook without hampering the customer experience or forcing the customer to crack the DRM in order to use an ebook on various devices. The publishers of ebooks would not likely be interested in suing their customers,[71] and therefore, the only purpose for using DRM

[69] Watermarks are not generally removable. However, a crafty programmer may be able to find a way to watermark "over" the existing watermark with a different image or with blank white or black space.

[70] Cory Verner is the founder and president of eChristian, Inc., a publisher of ebooks and audiobooks. Many thanks to Cory for his thoughts on this paper. I must give him credit for the invention of the idea of embedding the CMI into the PI watermark and for allowing me to include it in this paper.

[71] Suing customers is impractical and likely to include the wrong defendants, incur bad press, and overall fail a reasonable cost/benefit analysis.

would be to ensure that the publisher can, if necessary, seek remedies against secondary markets. Thus, ebook publishers need something that is "minimally DRM," and only sufficiently technical that the DRM will qualify for protection under the DMCA. The solution needs to be practical in the context of the exploding demand for ebooks. Ebooks need to be free of reader software and devices, but allow enforcement under the DMCA where necessary.

The proposed solution for DRM Lite would provide a minimal technical measure in a watermark that contains the user's personal information displayed in such a way that the user would not want to put the ebook into the hands of a third party. This, combined with terms of use in a clickwrap agreement would constitute a means of protection for ebook publishers that would be more effective than current DRM by actually doing something to prevent the consumer from selling the ebook. Yet, it would also provide a means of pursuing third-party used ebook stores, should the watermark be removed or obscured.