HOW TO CIRCUMVENT TECHNOLOGICAL PROTECTION MEASURES WITHOUT VIOLATING THE DMCA: AN EXAMINATION OF TECHNOLOGICAL PROTECTION MEASURES UNDER CURRENT LEGAL STANDARDS

Ryan Iwahashi[†]

In *MGE UPS Systems, Inc. v. GE Consumer and Industrial Inc.* (*MGE I*), the Fifth Circuit initially dismissed a circumvention claim by stressing that the Digital Millennium Copyright Act (DMCA) only protects "copyrighted material against infringement of a right that the Copyright Act protects, not from mere use or viewing."[1] Under this holding, circumventing a technological protection measure (TPM) only violates the DMCA if the TPM is circumvented to infringe a right protected by the Copyright Act. This narrow interpretation of the anti-circumvention provision caused a panic among copyright owners concerned about protecting against digital piracy.[2]

The Fifth Circuit has since amended its *MGE I* decision to omit this discussion of the DMCA and decided the case on other grounds.[3] Nevertheless, the initial decision illustrates the problem with the current judicial interpretations of the anti-circumvention clause. Under 17 U.S.C. § 1201(a)(1)(A), "No person shall circumvent a technological measure that *effectively controls access* to a work protected under [the Copyright Act]."[4] Since courts do not agree on the legal standard to apply in anti-circumvention

[†] J.D. Candidate, 2012, University of California, Berkeley School of Law.

[1] MGE UPS Sys., Inc. v. GE Consumer & Indus., Inc., No. 08-10521, 2010 WL 2820006, at *3 (5th Cir. July 20, 2010), *withdrawn*, 2010 WL 3769210 (5th Cir. Sept. 29, 2010).

[2] *See* Brief for Recording Industry Association of America, Entertainment Software Association, Business Software Alliance and Software and Information Industry Association as Amici Curiae Supporting Respondents, *MGE I*, No. 08-10521 (U.S. July 20, 2010), 2010 WL 2820006; Brief for Motion Picture Association of America Inc. as Amici Curiae Supporting Respondents, *MGE I*, No. 08-10521 (U.S. July 20, 2010), 2010 WL 2820006.

[3] MGE UPS Sys., Inc. v. GE Consumer and Indus., Inc. (*MGE II*), No. 08-10521, 2010 WL 3769210 (2010).

[4] 17 U.S.C. § 1201(a)(1)(A) (2006) (emphasis added).

cases,[5] it is unclear to many copyright owners whether their TPMs "effectively control access"[6] under the various legal standards.

This Note surveys the range of TPMs on the market and offers guidance on how the various legal standards currently used by courts to interpret the DMCA may apply to efforts to circumvent these TPMs. Part I provides an overview of the DMCA and TPMs. Part II then describes and categorizes the various legal standards that courts have used to decide anti-circumvention cases. Part III undertakes a technical examination of the most common technological measures used to protect copyrighted material. Based on these technical specifications, Part IV analyzes how each legal standard may be applied to the technological measures and assesses which are likely to constitute valid TPMs under each test.

I. OVERVIEW OF THE DMCA AND TECHNOLOGICAL PROTECTION MEASURES

In 1998, Congress enacted the "anti-circumvention" provisions of the DMCA, codified in § 1201 of the Copyright Act, to stop copyright infringers from defeating anti-piracy protections added to copyrighted works as well as to ban devices intended for that purpose.[7] Congress was responding to copyright owners' concerns that their works would be pirated in the networked digital world despite any protection measures they implemented.[8] Section 1201 prohibits two distinct things: (1) *acts* of circumvention and (2) the *trafficking* of tools and technologies used for circumvention.[9]

The prohibition against *acts* of circumvention prohibits the actual act of circumventing a TPM used by copyrighted owners to control access to their works.[10] For example, a user's act of circumventing the encryption on a DVD movie to make a copy for a friend would be an act of circumvention.[11]

[5] *Compare* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317–19 (S.D.N.Y. 2000), *aff'd*, Universal City Studios, Inc. v. Corely, 273 F.3d 429 (2d Cir. 2001), *with* Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1204 (Fed. Cir. 2004).

[6] 17 U.S.C. § 1201(a)(1)(A).

[7] 17 U.S.C. § 1201; *see* 144 Cong. Rec. H7093, H7094–95 (Aug. 4, 1998); S. REP. NO. 105-90, at 29 (1998); H.R. REP. NO. 105-551, pt. 1, at 18 (1998); H.R. REP. NO. 105-551, pt. 2, at 38 (1998).

[8] *See* JESSICA LITMAN, DIGITAL COPYRIGHT: PROTECTING INTELLECTUAL PROPERTY ON THE INTERNET 89–150 (2000).

[9] *See* 17 U.S.C. § 1201.

[10] 17 U.S.C. § 1201(a)(1).

[11] *See, e.g.*, 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085, 1104–05 (N.D. Cal. 2004); Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 346 (S.D.N.Y. 2000), *aff'd*, Universal City Studios, Inc. v. Corely, 273 F.3d 429 (2d Cir. 2001).

The prohibition against *trafficking* tools used for circumvention prohibits the manufacture, sale, distribution, or trafficking of tools and technologies that make circumvention possible.[12] For example, creating and marketing a program that allowed users to circumvent the encryption on DVD movies would be trafficking a tool used for circumvention.[13]

Even though the two prohibitions are distinct, the statutory language of the access and trafficking provisions are essentially the same. The access provision, "[n]o person shall circumvent a *technological measure that effectively controls access to a work protected under this title*,"[14] has the same essential elements as the trafficking provision, "[n]o person shall . . . traffic in any technology . . . for the purpose of circumventing a *technological measure that effectively controls access to a work protected under this title*."[15] Consequently, this Note will discuss violations of the anti-circumvention statute in general.

However, this Note will not discuss the copy control circumvention provision of the DMCA. The copy control circumvention provision prohibits "circumventing protection afforded by a technological measure that effectively protects a right of the copyright owner under this title."[16] Some of the tests discussed in Section II.B and II.C, *infra*, seem to read similar limitations into the anti-circumvention provisions, even though the wording of the statute does not require that the TPM "effectively protect[] a right of the copyright owner."[17] The issue of whether these judicial interpretations of the anti-circumvention provisions of the DMCA are correct is beyond the scope of this Note. Instead, this Note will focus only on how courts have interpreted the anti-circumvention act.

While the DMCA provides definitions for "circumvent[ing] a technological measure" and "effectively control[ling] access to a work," it does not provide an explicit definition of a TPM.[18] Both the prohibitions against acts of circumvention and trafficking tools of circumvention pertain to "circumventing a technological measure that effectively controls access to a work."[19] But courts have struggled to agree on what exactly qualifies as a

[12] *See* 17 U.S.C. §§ 1201(a)(2), (b).

[13] *See* 321 Studios 307, F. Supp. 2d at 1104–05; Reimerdes, 111 F. Supp. 2d at 317–19.

[14] 17 U.S.C. § 1201(a)(1)(A) (emphasis added).

[15] *Id.* (emphasis added).

[16] 17 U.S.C. § 1201(b)(1)(A).

[17] *Id.*

[18] *See* 17 U.S.C. § 1201(a)(3).

[19] 17 U.S.C. § 1201(a)(1)(A).

TPM.[20] Technology and circumvention techniques continue to evolve, and copyright owners employ a wide range of technological measures that are designed to prevent piracy in one form or another. Consequently, courts are forced to grapple with technically complex protection measures to determine if circumvention would amount to a violation of the DMCA.

However, not all technological measures are designed to prevent piracy. Companies also use technological measures to prevent competition and, in some instances, try to use the DMCA to maintain their monopolies.[21] For example, a garage door manufacturer sought to use the DMCA to prevent third-party garage door openers from allegedly "circumvent[ing]" its rolling code protection measure.[22] Using the anti-circumvention statute in this way stifles free speech, prevents competition, and threatens legitimate scientific research.[23] In resolving these disputes, courts have struggled to arrive at the results most in line with the legislative intent of the DMCA, without imposing liability where the technological measure was not actually designed to prevent piracy.[24] This effort by courts has produced a few distinct tests for determining when circumvention of a TPM actually violates the DMCA.

II. CURRENT LEGAL STANDARDS FOR TECHNOLOGICAL PROTECTION MEASURES

The cases that have decided whether a TPM is covered by the DMCA can be roughly split into distinct categories based on their use of four different tests: the Literal Interpretation Test, the Nexus Test, the Other Access Point Test, and the Permission or TPM Test. For a TPM to qualify under the text of the statute, it must be a technological measure that

[20] *Compare* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317–19 (S.D.N.Y. 2000), *aff'd*, Universal City Studios, Inc. v. Corely, 273 F.3d 429 (2d Cir. 2001), *with* Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1204 (Fed. Cir. 2004).

[21] *See* Davidson & Assocs. v. Jung, 422 F.3d 630, 633 (8th Cir. 2005) (trying to prevent compatibility of third party game servers); Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 546 (6th Cir. 2004) (trying to prevent compatibility of third party printer ink cartridges); *Chamberlain*, 381 F.3d at 1204 (trying to prevent compatibility of third party garage door openers).

[22] *See* Chamberlain, 381 F.3d at 1204 (noting that rolling code refers to code that changes at regular intervals).

[23] *See* Fred Von Lohmann, *Unintended Consequences: 12 Years Under the DMCA*, 1–2 (2010).

[24] *Compare Davidson*, 422 F.3d at 633 (holding that a competing game server did violate the DMCA), *with Lexmark*, 387 F.3d at 546 (holding that an ink cartridge competitor did not violate the DMCA), and *Chamberlain*, 381 F.3d at 1204 (holding that a garage door opener competitor did not violate the DMCA).

"effectively controls access" to a copyrighted work.[25] The DMCA explicitly states that "a technological measure 'effectively controls access to a work' if the measure, in the ordinary course of 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."[26]

A. LITERAL INTERPRETATION TEST

Courts adopting the broadest interpretation of the DMCA use the plain meaning of the text to impose liability on a circumventor of any TPM that "effectively controls access" to a copyrighted work.[27] This interpretation has been endorsed in the widest range of cases.[28]

For example, in *Universal City Studios, Inc. v. Reimerdes*, the court held that Content Scramble System (CSS) encryption, used to encrypt DVDs, was a valid TPM that effectively controls access to the work because "[o]ne cannot gain *access* to a CSS-protected work on a DVD without application of the three keys that are required by the software."[29] Since licensing arrangements carefully control access to these keys, obtaining one without permission amounts to an act of circumvention in violation of the DMCA.[30]

The Literal Interpretation test only requires that the TPM controls "access" to the copyrighted work in the ordinary course of its operation

[25] *See* 17 U.S.C. § 1201(a)(1)(A) (2006).

[26] 17 U.S.C. § 1201(a)(3)(B).

[27] *Id.*

[28] *See* Coxcom, Inc. v. Chaffee, 536 F.3d 101 (1st Cir. 2008) (holding that the filter used to block pay-per-view cable charges was a violation of the DMCA); Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 346 (S.D.N.Y. 2000), *aff'd*, Universal City Studios, Inc. v. Corely, 273 F.3d 429 (2d Cir. 2001) (holding that marketing DeCSS was a violation of the DMCA); MDY Indus., LLC v. Blizzard Entm't, Inc., 616 F. Supp. 2d 958, 975 (D. Ariz. 2009) (holding that the bot used in World of Warcraft designed to avoid detection by the scanners used to detect bots was a violation of the DMCA); Sony Computer Entm't Am., Inc. v. Divineo, Inc., 457 F. Supp. 2d 957, 968 (N.D. Cal. 2006) (holding that the manufacturer of mod chips that circumvented the authentication check on a video game console to allow for the playing of unauthorized games was liable under the DMCA trafficking provision); 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085, 1104–05 (N.D. Cal. 2004) (holding that decrypting DVDs was a violation of the DMCA); Pearl Inv., LLC v. Standard I/O, Inc., 257 F. Supp. 2d 326, 350 (D. Maine 2003) (holding that the circumvention of the encrypted and password-protected VPN was likely a violation of the DMCA); Realnetworks, Inc. v. Streambox, Inc., No. 2:99CV02070, 2000 WL 127311, at *6 (W.D. Wash. Jan. 18, 2000) (holding that the circumvention of a secret handshake was a violation of the DMCA); *see also* 2 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12A.03 (Matthew Bender, Rev. Ed. 2010).

[29] *Reimerdes*, 111 F. Supp. 2d at 371 (emphasis added).

[30] *Id.* at 308.

through the "application of information, a process, or a treatment."[31] This broad interpretation of the anti-circumvention provisions of the DMCA does not distinguish between different types of access.[32] Nimmer endorses such an expansive interpretation because the Copyright Act includes two separate violations: one that "effectively controls access to a work" and another that "protects a right of a copyright owner under [the Copyright Act]."[33] The separation of these two violations implies that circumventing access is sufficient to violate the "effectively controls access" part.[34] Consequently, under the broadest interpretation of the anti-circumvention provisions in the DMCA, the TPM only needs to effectively control *access* to a copyrighted work in the ordinary course of events.[35]

B. NEXUS TEST

Other courts have created the "Nexus Test" to evaluate whether a TPM falls under the DMCA, which seemingly reads an extra requirement into the statute.[36] Not only does the potential violator need to circumvent the TPM to *access* the work, he must also violate one of the *rights* of the copyright holder to be liable under the DMCA.[37]

For example, in *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, Chamberlain marketed a garage door opener that used a rolling code (code that changes at set intervals) to protect against intruders stealing the transmission frequency.[38] The rolling code also had the effect of preventing third party garage door opener manufacturers from competing since they did not know the rolling code algorithm.[39] Skylink figured out a clever way to

[31] 17 U.S.C. § 1201(a)(3)(B).

[32] For example, the test does not distinguish between read access, write access, or copy access.

[33] 17 U.S.C. § 1201(a)(2)(A), (b)(1)(A); NIMMER, *supra* note 28, § 12A.03.

[34] 17 U.S.C. § 1201(b)(1)(A); NIMMER, *supra* note 28, § 12A.03.

[35] *See Reimerdes*, 111 F. Supp. 2d at 317–19.

[36] *See MGE I*, No. 08-10521, 2010 WL 2820006, at *3 (5th Cir. July 20, 2010) (holding that hacking the program to circumvent the dongle check was not a violation of the DMCA), *withdrawn*, 2010 WL 3769210 (5th Cir. Sept. 29, 2010); Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1204 (Fed. Cir. 2004) (holding that circumvention of the rolling code garage door opener was not a violation of the DMCA); Ticketmaster L.L.C. v. RMG Techs., Inc., 507 F. Supp. 2d 1096, 1111–12 (C.D. Cal. 2007) (holding that the mechanism use to regulate ticket sales sufficiently controlled access to the copyright- protected website so there was a violation of the DMCA); DirectTV Inc. v. Little, No. CV-03-2407-RMW, 2004 WL 1811153, at *6 (N.D. Cal. Aug. 12, 2004) (holding that no factual disputes relating to the right of a copyright holder are disputed).

[37] *See Chamberlain*, 381 F.3d at 1197.

[38] *Id.* at 1183.

[39] *Id.* at 1184–85.

open Chamberlain rolling code doors by transmitting two frequencies at once.[40] Chamberlain sued Skylink, claiming that the rolling code was a TPM and Skylink violated the DMCA by circumventing the rolling code protection to "access" the underlying copyrighted computer program that opened the garage door.[41] The Federal Circuit held that the anti-circumvention act "prohibits only forms of access that bear a reasonable relationship to the protections that the Copyright Act otherwise affords copyright owners." [42] The court added that "[w]hile such a rule of reason may create some uncertainty and consume some judicial resources, it is the only meaningful reading of the statute."[43] Therefore, Skylink did not violate the DMCA since "Chamberlain neither alleged copyright infringement *nor explained how the access provided by* [Skylink's transmitter] *facilitates the infringement of any right that the Copyright Act protects*."[44]

In applying the Nexus Test set out in *Chamberlain*, the Fifth Circuit in *MGE I* recognized that "[t]he owner's technological measure must protect the copyrighted material against an infringement of a right that the Copyright Act protects, *not from mere use or viewing*."[45] In that case, plaintiff MGE alleged that GE circumvented a TPM by modifying the MGE-copyrighted software to skip the check for a valid dongle that was normally required before the program could run. The Fifth Circuit found that MGE placed "no encryption or other form of protection on the software itself to prevent copyright violations," and thus "[b]ecause the dongle does not protect against copyright violations, the mere fact that the dongle itself is circumvented does not give rise to a circumvention violation within the meaning of the DMCA."[46] The dongle protection system merely prevents initial access to the software, and does not prevent the software from being freely read and copied on the computer.[47] Therefore, the court held that GE did not violate the DMCA under the Nexus Test.

In summary, to prove a violation of the DMCA under the Nexus Test, the copyright holder must show that: (1) a technological measure was circumvented to "access" a copyrighted work *and* (2) the access to the

[40] *Id.*

[41] *Id.* at 1185.

[42] *Id.* at 1202–03.

[43] *Id.*

[44] *Id.* at 1204.

[45] *MGE I*, No. 08-10521, 2010 WL 2820006, at *3 (2010) (emphasis added) (citing *Chamberlain*, 381 F.3d at 1204).

[46] *Id.* at *3.

[47] *Id.*

copyrighted work bears a reasonable relationship to the protections of the Copyright Act.[48]

C. NARROWER STANDARDS: "OTHER ACCESS POINT" AND "PERMISSION OR TPM" TESTS

Other courts have read two different limitations into the anti-circumvention statute that are distinct from the Nexus Test.

In *Lexmark International, Inc. v. Static Control Components, Inc.*, the Sixth Circuit set forth the "Other Access Point Test."[49] Under this test, if there is another point of access to a copyrighted work, circumvention of a TPM to that copyrighted work is not a violation of the DMCA.[50] The defendant in *Lexmark International* manufactured third-party print cartridges for use with Lexmark printers that circumvented the device's printer verification that Lexmark manufactured the cartridges.[51] The court found that purchase of a Lexmark printer allows the user "access" to the programs loaded on the printer memory "with or without the benefit of the authentication sequence, and the data from the program may be translated into readable source code after which copies may be freely distributed."[52] The court held that the DMCA does not apply where the work is otherwise accessible:

> Just as one would not say that a lock on the back door of a house 'controls access' to a house whose front door does not contain a lock and just as one would not say that a lock on any door of a house 'controls access' to the house after its purchaser receives the key to the lock, it does not make sense to say that this provision of the DMCA applies to otherwise-readily-accessible copyrighted works.[53]

In this case, since the consumers were able to access the programs after their purchase, the defendant's circumvention of the technological measure was immaterial.[54]

The Southern District of New York court set forth the "Permission or TPM" test in *I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information*

[48] *Chamberlain*, 381 F.3d at 1202–03.

[49] *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 546 (6th Cir. 2004).

[50] *See id.*

[51] *Id.* at 546.

[52] *Id.*

[53] *Id.* at 547.

[54] *Id.*

Systems, Inc. [55] In order to violate the DMCA under the "Permission or TPM Test," a circumventor must bypass the TPM through "some alternate avenue of access not sponsored by the copyright owner (like a skeleton key, or neutralizing device)."[56] Alternatively, if the circumventor obtains access to the copyrighted material through a copyright owner-sponsored method, even if that access is illegally obtained, the circumventor is merely bypassing *permission* of the copyright owner and does not violate the DMCA[57] The *I.M.S.* defendant stole usernames and passwords to the plaintiff's system and used them to download copyrighted material from the Internet.[58] The court found that password protection was a valid TPM, but the defendant did not circumvent this TPM because it did not avoid or bypass the password check.[59] Instead, "[m]ore precisely and accurately, what the defendant avoided and bypassed was *permission* to engage and move through the technological measure from the measure's author."[60] Since the defendant used passwords "intentionally issued by the plaintiff to another entity," the TPM was not circumvented.[61]

Courts have taken a variety of approaches to their analysis of whether a given TPM is covered under the anti-circumvention provisions of the DMCA. Table 1 summarizes which courts have adopted the four legal tests.

[55] *See* I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 523 (S.D.N.Y. 2004).

[56] *Id.* at 533.

[57] *Id.* at 533–34.

[58] *Id.* at 523.

[59] *Id.* at 532.

[60] *Id.*

[61] *Id.* at 532–33.

Table 1: DMCA Anti-Circumvention Decisions Classified by Legal Standard

Literal Interpretation Test	1st Circuit[62] S.D.N.Y. affirmed by 2nd Circuit[63] N.D. Cal.[64] D. Arizona[65] D. Maine[66] W.D. Wash.[67]
Nexus Test	Federal Circuit[68] 5th Circuit (withdrawn)[69] C.D. Cal.[70] N.D. Cal.[71]
Other Access Point Test	6th Circuit[72]
Permission or TPM Test	S.D.N.Y.[73]

III. COMMON TECHNOLOGICAL PROTECTION MEASURES

This Part will provide a high level overview of some of the most common TPMs used by copyright holders. The technical details provided for each TPM provide necessary background for the later discussion, *infra* Part

[62] Coxcom, Inc. v. Chaffee, 536 F.3d 101 (1st Cir. 2008).

[63] Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317–19 (S.D.N.Y. 2000), *aff'd*, Universal City Studios, Inc. v. Corely, 273 F.3d 429 (2d Cir. 2001).

[64] Sony Computer Entm't Am., Inc., 457 F. Supp. 2d 957 (N.D. Cal. 2006); 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085 (N.D. Cal. 2004).

[65] MDY Indus., LLC v. Blizzard Entm't, Inc., 616 F. Supp. 2d (D. Ariz. 2009).

[66] Pearl Inv., LLC v. Standard I/O, Inc., 257 F. Supp. 2d 326 (D. Maine 2003).

[67] Realnetworks, Inc. v. Streambox, Inc., No. 2:99CV02070, 2000 WL 127311 (W.D. Wash. Jan. 18, 2000).

[68] Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178 (Fed. Cir. 2004); Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc., 431 F.3d 1307 (Fed. Cir. 2005).

[69] *MGE I*, No. 08-10521, 2010 WL 2820006, at *3 (5th Cir. July 20, 2010), *withdrawn*, 2010 WL 3769210 (5th Cir. Sept. 29, 2010). Since this case was decided on other grounds, the initial opinion that used the Nexus Test was withdrawn.

[70] Ticketmaster L.L.C. v. RMG Techs., Inc., 507 F. Supp. 2d 1096 (C.D. Cal. 2007).

[71] DirectTV Inc. v. Little, No. CV-03-2407-RMW, 2004 WL 1811153 (N.D. Cal. Aug. 12, 2004).

[72] Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 547 (6th Cir. 2004).

[73] I.M.S. Inquiry Mgmt. Sys., LTD. V. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 523 (S.D.N.Y. 2004).

IV, of how courts' varied legal interpretations of the DMCA might be applied to each measure.

A. PASSWORD PROTECTION

Password protection is the most common and well-known TPM. Passwords are used to control access to all kinds of copyrighted works, from high-priced software to personal emails. Exactly what kind of access a password protects depends on where the copyrighted work is stored.

If the copyrighted work is stored on a hard drive, the password prompt will typically be invoked whenever the processing unit is trying to read the file.[74] For example, this situation could apply to a document stored on a user's hard drive. The user will not be able to view the data without either entering the password or circumventing the password prompt.[75] However, this password prompt provides no protection against copying the file. A user can still copy the file to any other location, although the copy will still prompt the user for a password when it is opened. To bypass the password prompt, a circumventor will simply use an application that does not check for password protection or hack the application to not prompt for a password. Alternatively, the circumventor can also just use a "brute force attack," meaning that he can keep guessing passwords until he determines the correct one. If the copyrighted work is stored on external media, the password prompt will typically be invoked when the external media is attached to the computer.[76] A software program that cannot be installed on a user's computer unless a key or password is entered is an example of a password-protected work stored on external media. Conceptually, the accessibility of the file and list of potential attacks are the same as if the file were stored on the user's computer.[77]

If the copyrighted work is stored in a remote location over the Internet, the password prompt will appear when the remote location is first accessed. For example, a web-based email account would fall into this category. The user will not be able to access the copyrighted material without a proper password. In other words, none of the copyrighted work will be transmitted to the user unless a proper password is inputted.[78] This prevents the user

[74] *See* MATT BISHOP, COMPUTER SECURITY: ART AND SCIENCE 310–22 (2003); Daniel V. Klein, *"Foiling the Cracker": A Survey of, and Improvements to, Password Security*, Proceedings of the 14th DoE Computer Security Group (1991) 1–2.

[75] *See* Klein, *supra* note 74, at 2.

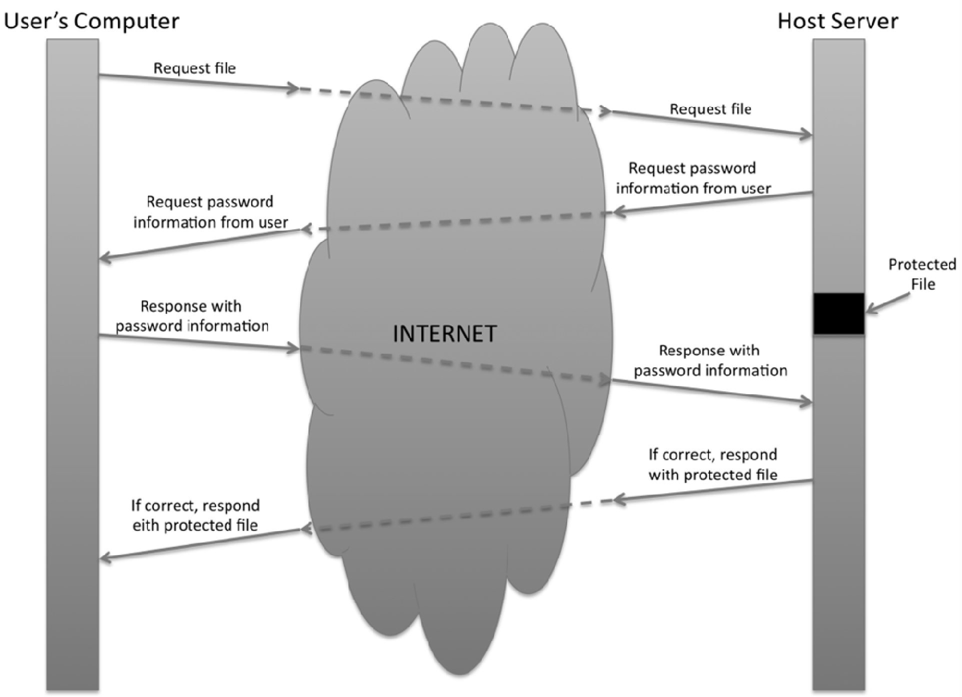
[76] *See id.*

[77] BISHOP, *supra* note 74, at 310–22.

[78] *See* Klein, *supra* note 74, at 2.

from accessing the copyrighted work, but also prevents any form of copying of the work. The typical way to circumvent this type of password protection is to obtain the user's password illegally or guess the user's password using a brute force attack.[79] Figure 1 diagrams how this process works, starting with the user requesting the file through the Internet and ending with the protected file being transferred to the user if the password is correct.

Figure 1: Password-Protected File Stored in a Remote Location


User's Computer
Host Server
Request file
Request file
Request password information from user
Request password information from user
Protected File
Response with password information
INTERNET
Response with password information
If correct, respond with protected file
If correct, respond eith protected file

B. DONGLES

Dongles are USB keys that are equipped with security information and attached to the computers of software customers to protect the software from being exploited.[80] The software is designed to run only if it finds the corresponding dongle is physically attached to the user's computer.[81] The protected software will be installed on the user's computer in two pieces: (1) the protected software portion; and (2) the dongle application programming interface (API), which can be thought of as the unprotected portion of the

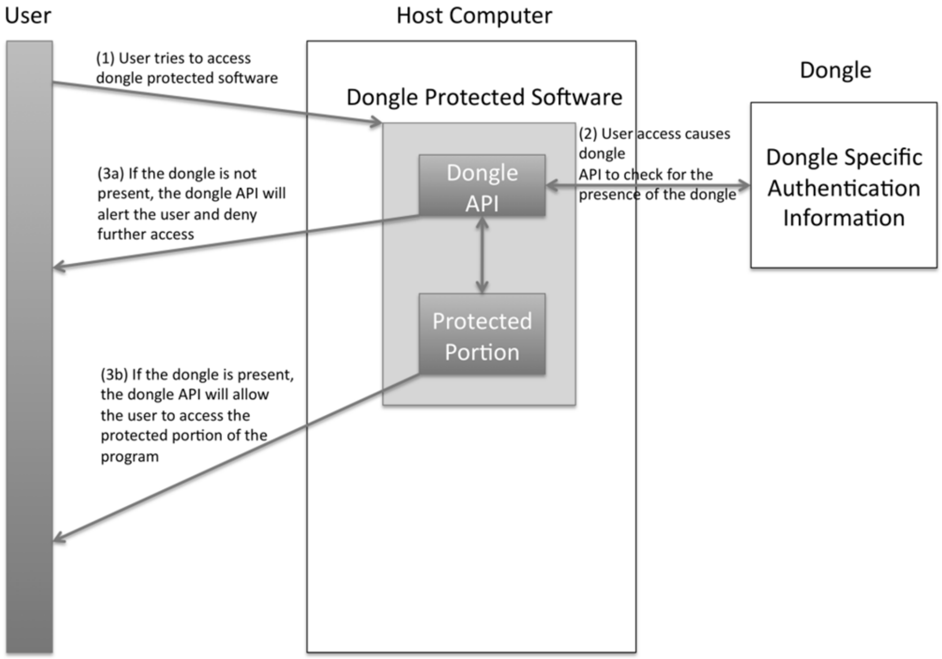
[79] BISHOP, *supra* note 74, at 310–22.

[80] Ugo Piazzalunga et. al, *Security Strength Measurement for Dongle-Protected Software*, IEEE Security & Privacy, November/December 2007, at 32.

[81] *Id.*

software.[82] When the protected program is launched, the unprotected API will be the first application launched. The API will not permit access to the protected code unless the dongle is plugged into the user's computer.[83] Dongles successfully prevent the protected code from being run on the computer because the dongle API must successfully detect the presence of a dongle before the protected code is triggered. However, even though the dongle API will prevent the code from being run if the dongle is not present, a dongle does not prevent the protected code from being copied. Even the protected portion of the code is just stored on the user's computer and the program can be freely copied using other applications. Figure 2 shows the conceptual separation between the dongle API and the protected portion of the code.

Figure 2: Dongle-Protected Software Authentication System


User
Host Computer
(1) User tries to access dongle protected software
Dongle Protected Software
Dongle
(2) User access causes dongle API to check for the presence of the dongle
Dongle API
Dongle Specific Authentication Information
(3a) If the dongle is not present, the dongle API will alert the user and deny further access
Protected Portion
(3b) If the dongle is present, the dongle API will allow the user to access the protected portion of the program

The typical way to circumvent the dongle check is to hack the dongle API code. The hacked dongle API will just bypass the actual check for the dongle and start the protected program as if the dongle were present.[84] This

[82] *Id.*

[83] *Id.*

[84] *See MGE I*, No. 08-10521, 2010 WL 2820006, at *3 (2010).

will allow the user to access the protected software without having the dongle plugged in.

C. ENCRYPTION

As there are many different forms of encryption, this discussion focuses on the encryption technique behind the best-known example of an encrypted copyrighted work, the DVD.[85] The content scrambling system (CSS) algorithm encrypts each DVD, which prevents reading by unlicensed players. The encrypted DVD is unusable and unplayable to any user unless the content is first decrypted. DVDs actually use several layers of encryption to prevent unlicensed players from reading the copyrighted material on the disc.[86] The video content of every DVD is encrypted with a unique title key that is stored directly on the disk.[87] Then the title key is encrypted on the DVD using player keys that are assigned to licensed manufacturers of DVD players.[88] Each player key is assigned to manufacturers after they agree to the licensing terms. The title keys encrypted by all of the different player keys are stored in the "Media Key Block" ("MKB") portion of the disk.[89] Once the title key is decrypted by the player using the assigned player key, this title key is sent through a pre-defined function known by a licensed DVD player. This function is known as a hash function, and is irreversible so that a circumventor cannot calculate the title key from the correct hash value stored on the DVD.[90] The result of this hash function is then compared to the correct hash key on the DVD to make sure the player obtained the correct title key.[91] Only then can the title key be used to decrypt the content of the DVD. Copyright holders can control the copying of the DVD because any manufacturer that licenses CSS must agree to disallow copying on their player.[92] Also, there is nothing to prevent the entire encrypted disk from being copied using an unlicensed DVD player that can read the data on the computer; however, the copy will also be encrypted.[93] Figure 3 shows how this DVD decryption process works.

[85] BISHOP, *supra* note 74, at 215–71.

[86] L Jean Camp, *DRM: Doesn't Really Mean Digital Copyright Management*, IEEE Internet Computing, May 2003, at 78.

[87] *Id.*

[88] *Id.*

[89] *Id.*

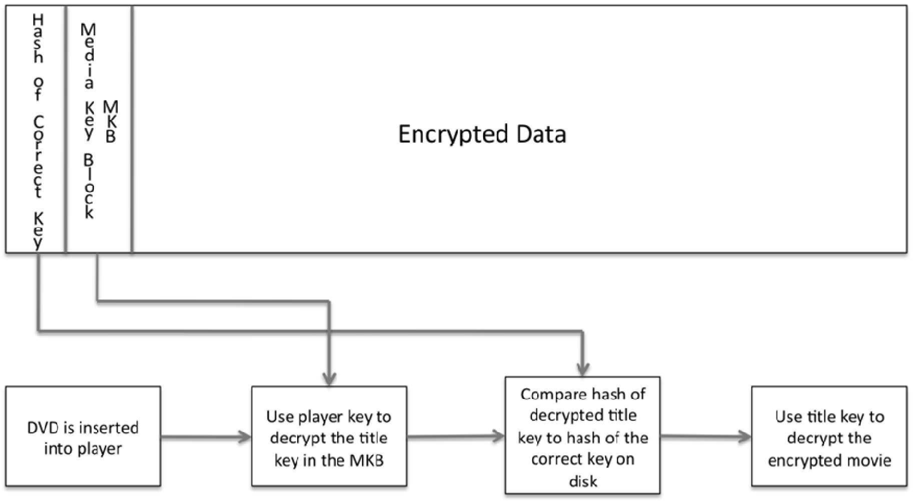
[90] MARK ALLEN WEISS, DATA STRUCTURES & ALGORITHM ANALYSIS IN C++ 181–84 (1999).

[91] Camp, *supra* note 86, at 78; *see* WEISS, *supra* note 90, at 181–84.

[92] Camp, *supra* note 86, at 78.

[93] *Id.*

Figure 3: Normal Decryption Process of a DVD Movie


Hash of Correct Key
Media Key Block
MKB
Encrypted Data
DVD is inserted into player
Use player key to decrypt the title key in the MKB
Compare hash of decrypted title key to hash of the correct key on disk
Use title key to decrypt the encrypted movie

Controlling the decryption key is the most important part of controlling the encrypted copyrighted work. DVDs control their keys using licensing, but keys can also be stored on dongles or controlled over the Internet. Circumventing encryption almost always involves discovering the decryption keys. DeCSS is an algorithm that broke the encryption on DVDs by stealing a valid player key to extract the title key.[94] However, encryption can also always be broken by a brute force attack. With the speed of today's computers, it is possible to try every possible decryption key to a DVD relatively quickly.[95]

D. REGION CODING

In addition to encryption, region coding is also used on DVDs. The region coding system prevents people from playing foreign DVDs on their DVD players.[96] In order to take advantage of price differentiation in the global economy, DVD manufacturers added a region coding flag to DVDs

[94] The Openlaw DVD/DECSS Forum Frequently Asked Questions (FAQ) List, http://cyber.law.harvard.edu/openlaw/DVD/dvd-discuss-faq.html (last visited Nov. 19, 2010).

[95] Matthew Becker & Ahmed Desoky, *A Study of the DVD Content Scrambling System (CSS) Algorithm*, Proceedings of the Fourth IEEE Int'l Symposium on Signal Processing and Information Technology (2004).

[96] Qixiang Sun, *The DMCA Anti-Circumvention Provisions and the Region Coding System: Are Muti-Zone DVD Players Illegal After the* Chamberlain *and* Lexmark *Cases?*, 2005 J.L. TECH. & POL'Y 317, 317–18 (2005).

that indicates which region the disk was purchased in.[97] DVD players then check for the existence of this flag and refuse to play it if it is not from an authorized region. Regional coding does not utilize encryption; this is merely a flag that gets checked when the DVD is loaded.[98]

The region code check can be easily circumvented by either purchasing a multi-zone DVD player or modifying a DVD player to skip the region code check.

E. ONLINE MOVIE RENTAL PROTECTION

iTunes and other online providers now allow users to "rent" movies over the Internet for a limited period of time by using a technical protection measure. After the time of the rental, the movie will automatically delete itself from the user's computer. For iTunes, a rented movie will be automatically deleted thirty days after it is downloaded, or twenty-four hours after the user starts watching it.[99] This effect is done with the Moving Picture Expert Group Rights Expression Language (MPEG REL).[100] MPEG REL is a standardized rights expression language that enables the controlled distribution of and access to digital content.[101] It works by associating an XML header, extra metadata, with each file that will be controlled by MPEG REL.[102] The header contains a standardized definition of the rights associated with the file for the user. Each copyrighted file is still stored as data on the user's computer, but with a MPEG REL header attached. This means the data can still be copied and accessed from other applications. Furthermore, copying is explicitly allowed during the rental period so a user can watch the movie on other devices. Additionally, the addition of the MPEG REL header does not allow the file to just delete itself. The deletion of the file after it has expired relies on another application, such as iTunes, to actively delete the file.

Mechanism for online movie rental protection can be circumvented using a few different methods. An early circumvention technique to extend the length of movie rentals has since been fixed, but it makes an interesting

[97] *Id.*

[98] *Id.*

[99] *iTunes Store: Movie Rental Frequently Asked Questions*, APPLE.COM, http://support.apple.com/kb/HT1657?viewlocale=en_US (last visited November 18, 2010).

[100] Xin Wang et al., *The MPEG-21 Rights Expression Language And Rights Data Dictionary*, 7 IEEE Transactions on Multimedia 408, 408–09 (June 2005).

[101] *Id.*

[102] *Id.*

circumvention example.[103] Before renting a movie, the circumventor would set his computer clock ahead by about twenty years. He would subsequently rent the movie and start viewing it and then set his clock back to today's date. This made the rental period last for twenty years instead of the typical thirty days.[104]

F. SECRET HANDSHAKES

The *RealNetworks, Inc. v. Streambox, Inc.* case involved the use of a "secret handshake" between the RealNetworks servers and their user application to play music streamed from the servers.[105] In order to prevent copying of copyrighted music, RealNetworks set up a secret handshake protocol between an authorized user application and the server so that music could only be streamed directly to the authorized user application that did not allow copying.[106]

There are a number of different "secret handshake" protocols, but most of them involve a challenge response sequence to authenticate the user. First, the user will initiate the connection and identify itself to the server. Then the server will send a challenge message to the user consisting of a random number.[107] The user will have to put the random number through a predefined hash function and send the result back to the server.[108] The server will compare the user's response with its own hash calculation. If the two values match then the user will be authenticated.[109] Without completing the secret handshake, the user will not be able to view or copy the copyrighted work. The data is stored on the server and will not be sent if the secret handshake protocol fails. Figure 4 shows how this secret handshake works.

[103] *See* Matt Buchanan, *Confirmed: Change Your System Time, Watch Your iTunes Rentals Forever*, GIZMODO.COM (Jan. 17, 2008, 10:30 AM), http://gizmodo.com/345964/confirmed-you-can-keep-your-itunes-movie-rentals-for-eternity-but-it-aint-easy.

[104] *Id.*

[105] Realnetworks, Inc. v. Streambox, Inc., No. 2:99CV02070, 2000 WL 127311, *2–3 (W.D. Wash. Jan. 18, 2000).

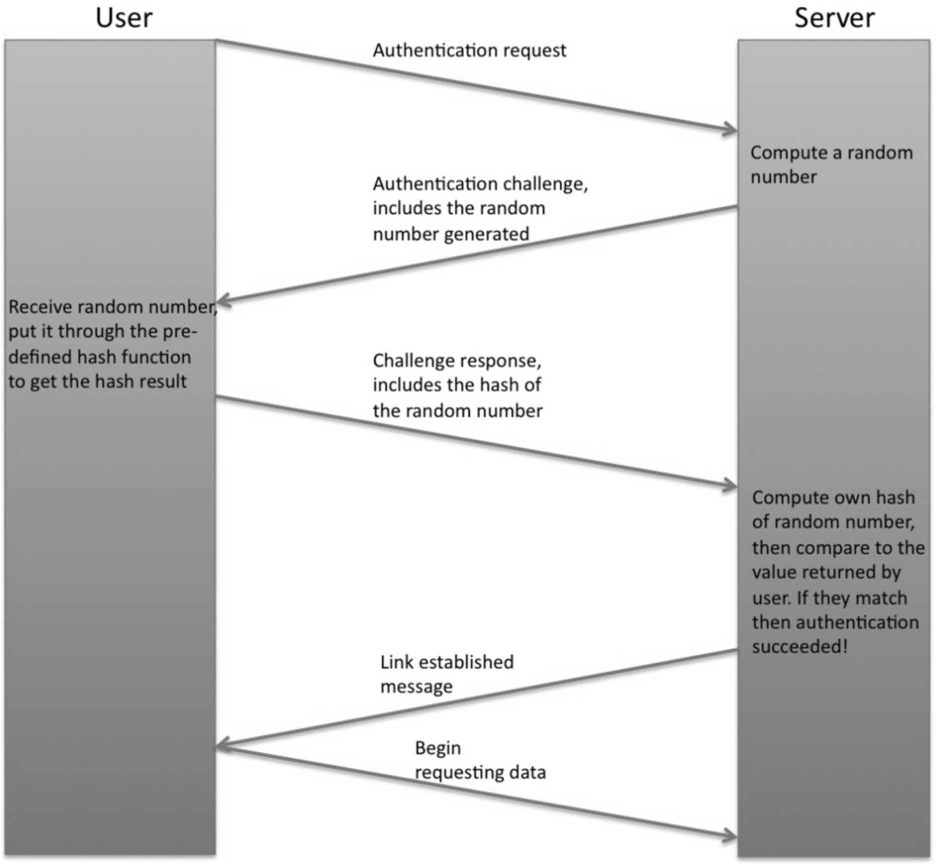
[106] *Id.* at *2–3.

[107] BISHOP, *supra* note 74, at 324–28; D.W. DAVIES & W.L. PRICE, SECURITY FOR COMPUTER NETWORKS: AN INTRODUCTION TO DATA SECURITY IN TELEPROCESSING AND ELECTRONIC FUNDS TRANSFER 185 (2nd ed. 1989).

[108] DAVIES, *supra* note 107, at 185.

[109] *Id.*

Figure 4: Challenge Response Secret Handshake Protocol


User
Server
Authentication request
Compute a random number
Authentication challenge, includes the random number generated
Receive random number, put it through the pre-defined hash function to get the hash result
Challenge response, includes the hash of the random number
Compute own hash of random number, then compare to the value returned by user. If they match then authentication succeeded!
Link established message
Begin requesting data

There are many ways to circumvent a handshake protocol. The defendant in the RealNetworks case created his own user application that mimicked the handshake protocol of the authentic user application, which requires knowing the hash function that is used by the server.[110] The easiest way to circumvent a secret handshake is a man-in-the-middle attack.[111] The circumventor will open up a connection with the server and the client and pretend to be the other with each. When the server challenges the client, the circumventor will receive the challenge from the server and forward it on to the client. The client will then send the correct response to the circumventor, who will forward it to the server.[112] At this point, the server will open up a connection directly with the circumventor and stream copyrighted data right

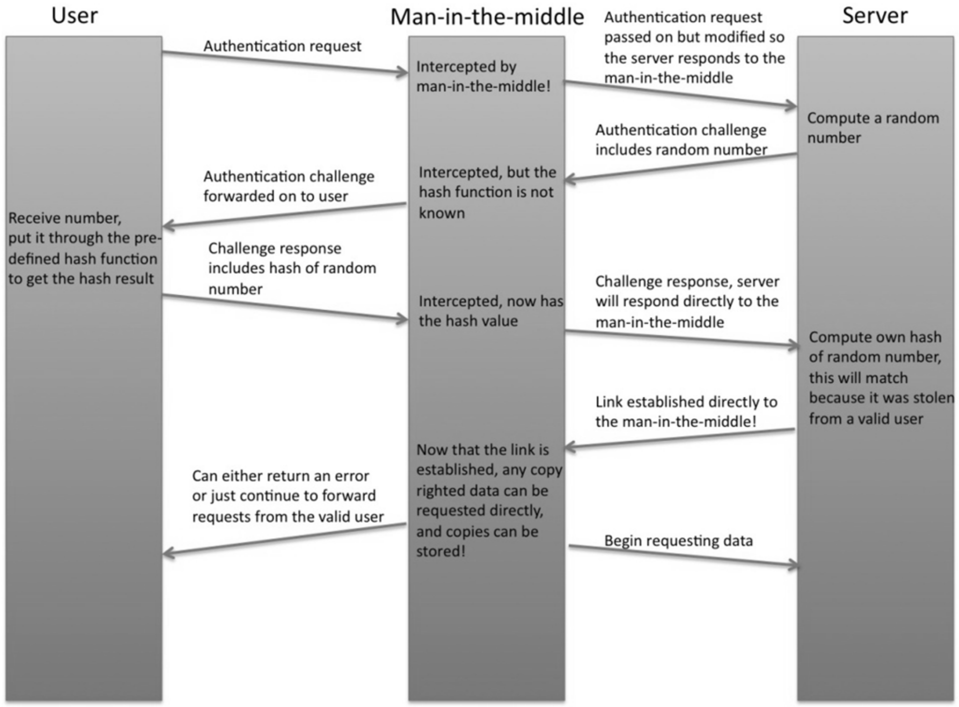
[110] *RealNetworks*, 2000 WL at *4–5.

[111] BISHOP, *supra* note 74, at 324–28; N. Asokan et al., *Man-in-the-Middle in Tunneled Authentication Protocols*, 3364 LECTURE NOTES IN COMPUTER SCIENCE 28, 28–29 (2005).

[112] BISHOP, *supra* note 74, at 324–28; Asokan, *supra* note 111, at 28.

to the circumventor. This will allow the circumventor direct access to the copyrighted material rather than through the authorized user application that prevents copying.[113] Figure 5 shows the how a typical man-in-the-middle attack works.

Figure 5: Challenge Response Protocol Circumvented by Man-in-the-Middle Attack


User
Man-in-the-middle
Server
Authentication request
Intercepted by man-in-the-middle!
Authentication request passed on but modified so the server responds to the man-in-the-middle
Compute a random number
Authentication challenge includes random number
Intercepted, but the hash function is not known
Authentication challenge forwarded on to user
Receive number, put it through the pre-defined hash function to get the hash result
Challenge response includes hash of random number
Intercepted, now has the hash value
Challenge response, server will respond directly to the man-in-the-middle
Compute own hash of random number, this will match because it was stolen from a valid user
Link established directly to the man-in-the-middle!
Now that the link is established, any copy righted data can be requested directly, and copies can be stored!
Can either return an error or just continue to forward requests from the valid user
Begin requesting data

G. WATERMARKING AND ANALOG COPY PROTECTION

Watermarks and Analog Copy Protections (ACP) both work by adding a signal to the output of an audiovisual copyrighted work.[114] It is important to note that neither process actually prevents copying or viewing of the copyrighted work. Both processes merely add extra data to the copyrighted work to discourage or track unauthorized copies.

[113] *See RealNetworks*, 2000 WL at *4–5.

[114] Maurice Maes et al., *Digital Watermarking DVD Video Copy Protection: What Issues Play a Role in Designing an Effective System?*, IEEE Signal Processing Magazine (2000), at 2; A. Eskicioglu & E. Delp, *An Overview of Multimedia Content Protection in Consumer Electronics Devices*, 16 SIGNAL PROCESSING: IMAGE COMMUNICATION 681, 682–83 (2001).

Watermarking adds an undetectable signal, called a watermark, to the work.[115] This means all of the copies will include this undetectable watermark as well.[116] These watermarks are typically designed to be unique for every legal copy. This means that whenever an illegal copy is found it can be traced back to a single legal source to identify the copyright infringer.[117] Depending on the type of watermarking technique used, there are a variety of different ways to remove the watermark in any copies to prevent identification of the infringer.[118]

ACP works by adding a signal to the outgoing stream of digital media, like DVDs, which makes it impossible for a viewer to watch an analog copy.[119] ACP does not prevent copying of the underlying work; it merely adds an extra layer of data to make analog copies unusable.[120] Even though an analog copy will be unwatchable in analog, there are devices that digitize the analog video, which removes the extra ACP data and allows for clear viewing.[121]

IV. CLASSIFICATION OF THE TPMS BASED ON VARIOUS LEGAL STANDARDS OF CIRCUMVENTION

This Part will classify the TPMs that were discussed in Part III, *supra*, based on the four legal standards discussed in Part II, *supra*. For analytical purposes, each of the following Sections assume that the technological measure being analyzed is the only measure utilized to control access to the copyrighted work. In practice, however, multiple measures are typically employed to protect a single work. For example, encryption and region coding protect DVD movies, and dongles are often used as the storage location for an encryption key.

A. PASSWORD PROTECTION

This Section analyzes a circumventor's effort to bypass the password check by obtaining a valid password either through brute-force guessing or

[115] Maes et al., *supra* note 114, at 2–4.

[116] *Id.*

[117] *Id.*

[118] *See id.*; *see also* JT Smith, *Felten SDMI Presentation: No Cops, but Lingering Questions about the DMCA*, LINUX.COM (August 16, 2001, 8:00 AM), http://www.linux.com/archive/feed/15591.

[119] Eskicioglu & Delp, *supra* note 114, at 682.

[120] *Id.*

[121] Nate Anderson, *Digitalizing Video Might Violate the DMCA*, ARS TECHNICA (Aug. 16, 2006), http://arstechnica.com/old/content/2006/08/7517.ars.

stealing an authorized user's password. It is also possible to use a hack to bypass the password check if the application is installed locally, but this circumvention technique is similar to the dongle hack described in Section IV.B., *infra*.

1. *Literal Interpretation Test*

Since under this legal standard the TPM only needs to effectively control *access* to a copyrighted work,[122] circumvention of the password check by illegally obtaining a valid password is likely a violation of the anti-circumvention statute. The password check is a technological measure that "effectively controls access to a work" because it requires the application of information, the password, to gain access to the work.[123] Just as use of an illegally obtained player key to read a DVD was a violation of the DMCA in *Reimerdes*, use of an illegally obtained password is a violation of the DMCA under the Literal Interpretation Test.[124]

2. *Nexus Test*

According to the Nexus test, the copyright holder must show that: (1) a technological measure was circumvented to "access" a copyrighted work *and* (2) the access to the copyrighted work bears a reasonable relationship to the protections of the Copyright Act.[125] The first prong of the test was just analyzed in Section IV.A.1., *supra*, so the remaining issue is whether the access bears a reasonable relationship to the protections of the Copyright Act. Just like the dongle in *MGE I*, the password prompt merely prevents initial access to the copyrighted work.[126] If the work is stored locally, it can be freely copied or distributed without the consumer being prompted for a password. Furthermore, if the data is stored on removable media, the entire contents of the media can be copied locally without entering a password. This is because it is the accessing application that checks to see if the password is required. Since the file is available locally, a circumventor can simply copy the file without accessing the application that checks for a password. As in *Chamberlain*, where the rolling code did not protect any of

[122] Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317–19 (S.D.N.Y. 2000), *aff'd*, Universal City Studios, Inc. v. Corely, 273 F.3d 429 (2d Cir. 2001).

[123] *See* 17 U.S.C. § 1201(a)(3)(B) (2006).

[124] *See Reimerdes*, 111 F. Supp. 2d at 317–19.

[125] Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1203 (Fed. Cir. 2004).

[126] *See* MGE I, No. 08-10521, 2010 WL 2820006 (5th Cir. July 20, 2010) *withdrawn* 2010 WL 3769210 (5th Cir. Sept. 29, 2010).

the copyright holder's rights, the password prompt does not prevent copying or distribution at all.[127]

However, if the copyrighted work is stored remotely, the work cannot be copied or distributed without the password because it is not stored on the user's computer. Unlike when the protected file is stored locally, remote storage prevents copying and distribution without a valid password. Therefore, circumventing password protection likely only violates the DMCA under the Nexus Test if the copyrighted work is stored in a remote location, instead of locally or on any accessible removable media.

3. *Other Access Point Test*

Although the password prompt prevents access to the copyrighted work through normal access, there are many other access points to the work, regardless of whether it is stored locally or on external media. Just as in *Lexmark* where the code on the print cartridge was freely accessible to the user, here, the works can be copied and distributed directly by the user without need for a password.[128] Therefore, this will probably not constitute violation of the DMCA. However, if the work is stored remotely, the only means of accessing the work is through the password prompt. Circumventing password protection on data stored remotely likely constitutes a violation of the DMCA under the Other Access Point Test.

4. *Permission or TPM Test*

The Permission or TPM Test relies on the distinction between circumventing the permission to access the work versus circumventing the actual TPM. If a circumventor uses a copyright holder-sanctioned method of accessing the work, then only the permission is being circumvented and there is no violation of the DMCA. Here, the circumventor is using a valid, but illegally obtained, password. This is the exact scenario in *I.M.S. Inquiry Management Systems,*[129] in which the court held that illegally obtaining an otherwise legitimate user's password is not a violation of the DMCA.[130]

[127] *See Chamberlain*, 381 F.3d at 1203–04.

[128] *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 547 (6th Cir. 2004).

[129] I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 532–33 (S.D.N.Y. 2004).

[130] *See* discussion, *supra*, Section IV.C.

B. DONGLES

This Section analyzes the circumvention method of hacking the dongle API program such that the program always returns that a valid dongle is present.

1. *Literal Interpretation Test*

Since under this legal standard the TPM only needs to effectively control *access* to a copyrighted work,[131] circumvention of the dongle by hacking the dongle API to always return that a valid dongle is present will likely constitute a violation of the DMCA. The use of a dongle to restrict access to a software program is a technological measure that "effectively controls access to a work" because the measure requires checking for a dongle implemented by the dongle API before a user can gain access.[132] Similar to *Reimerdes*, where the unauthorized use of a player key to obtain access to the copyrighted work was a violation of the DMCA, unauthorized hacking of the dongle API likely violates the DMCA.[133]

2. *Nexus Test*

The first prong of the Nexus Test was analyzed in the previous Section IV.B.I, so the remaining issue is whether the access bears a reasonable relationship to the protections of the Copyright Act. Since the program initiating the dongle check is stored locally, it can easily be copied or accessed through other means. This is the exact scenario set forth in *MGE I*, where circumventing the dongle did not constitute a violation of the DMCA under the Nexus Test because the dongle merely prevented initial access and did not protect against copyright violations.[134]

3. *Other Access Point Test*

Even though the dongle check prevents access to the copyrighted software program through normal access to the program, there are other ways to access the program since the work is stored locally on the machine. The program can be freely copied without triggering the dongle check. Just as the *Lexmark* user had another point of access in his permission to access the copyrighted work on his printer after purchase, the dongle protection

[131] Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317–19 (S.D.N.Y. 2000), *aff'd*, Universal City Studios, Inc. v. Corely, 273 F.3d 429 (2d Cir. 2001).

[132] *See* 17 U.S.C. § 1201(a)(3)(B) (2006).

[133] *See* Universal City Studios, 111 F. Supp. 2d at 317–19.

[134] *See* MGE I, No. 08-10521, 2010 WL 2820006, *3 (2010).

measure allows other access points to the copyrighted work.[135] Consequently, circumventing the dongle check is likely not a violation of the DMCA based on the Other Access Point Test.

4. *Permission or TPM Test*

If the dongle was stolen from someone else and used, this would be equivalent to stealing someone's password. Under *I.M.S.,* that would probably not violate the DMCA.[136] However, hacking the unprotected part of the code to circumvent the dongle check modifies the dongle API to provide an alternative access point not sanctioned by the copyright holder.[137] Consequently, the circumvention of the dongle check is probably a violation of the DMCA.

C. ENCRYPTION

This Section analyzes the use of a basic brute force attack to find the correct decryption key. This means that in order to circumvent the encryption, an attacker will try all possible keys until he finds the correct one. Once he has the correct key, he can decrypt and read the protected content.[138]

1. *Literal Interpretation Test*

Since under this legal standard the TPM only needs to effectively control *access* to a copyrighted work, circumventing the encryption by trying all of the possible decryption keys will constitute a violation of the DMCA.[139] A similar issue was decided in *Reimerdes*, where DeCSS was held to violate the DMCA because it bypassed CSS by using an illegally obtained player key.[140] The key could just as easily have been determined using a brute force attack.

[135] *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 547 (6th Cir. 2004).

[136] *See* I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 532–33 (S.D.N.Y. 2004).

[137] *See id.*

[138] The DeCSS algorithm decrypts DVDs by illegally obtaining a valid player key, so it does not need to run a brute force attack to extract a valid key. *See* The Openlaw DVD/DECSS Forum Frequently Asked Questions (FAQ) List, http://cyber.law.harvard.edu/openlaw/DVD/dvd-discuss-faq.html (last visited Nov. 19, 2010).

[139] *See* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317–19 (S.D.N.Y. 2000), *aff'd*, Universal City Studios, Inc. v. Corely, 273 F.3d 429 (2d Cir. 2001).

[140] *Id.*

2. *Nexus Test*

As the first prong of the test was analyzed in the previous Section IV.C.2, the remaining issue is whether the access bears a reasonable relationship to the protections of the Copyright Act.[141] Even though the copyrighted work is encrypted, that protection measure does not prevent the copying of the encrypted work. Since it is not clear whether copying the encrypted version of a work is a copying under the Copyright Act, liability under the Nexus Test would depend on a court's interpretation of "reproduce the copyrighted work."[142] It is unclear whether a reproduction can be made of a work that is still encrypted.[143]

If copying an encrypted work does not constitute making a copy within the protections of the Copyright Act, then encryption is not reasonably related to a right of the copyright holder. Just like in *Chamberlain*, where the rolling code did not protect any of the copyright holder's rights, the protection provided by encryption is not reasonably related to the protections of the Copyright Act.[144] Therefore, there is probably no violation of the DMCA. Conversely, if copying an encrypted file is considered making a copy under the Copyright Act, decrypting the encryption likely amounts to a violation of the DMCA under the Nexus Test.[145]

3. *Other Access Point Test*

The only way to access an encrypted copyrighted work is to decrypt it. Unlike *Lexmark*, where the user was able to access the unencrypted copyrighted work freely, there are no other points of access to an encrypted work without decrypting it first.[146] As a result, circumventing the encryption TPM likely constitutes a violation of the DMCA under the Other Access Point Test.

[141] Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1203 (Fed. Cir. 2004).

[142] 17 U.S.C. § 106(1) (2006).

[143] *See, e.g.*, 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 308 F. Supp. 2d 1085, 1098 (N.D. Cal. 2004) (noting that copying the work while it is still encrypted can be done, but is "not particularly useful").

[144] *See Chamberlain*, Inc., 381 F.3d at 1203.

[145] This seems to be the likely result based on *MGE I*, where the court implied that the result would be different if the software protected by the dongle was encrypted as well. MGE I, No. 08-10521, 2010 WL 2820006, *7 (5th Cir. July 20, 2010) *withdrawn* 2010 WL 3769210 (5th Cir. Sept. 29, 2010).

[146] *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 547 (6th Cir. 2004).

4. *Permission or TPM Test*

Since a brute force attack to break encryption involves trying all of the possible keys until the circumventor finds the correct key, the circumventor is actually using the copyright holder's sanctioned method of accessing the content.[147] Just like using an illegally obtained but valid password in *I.M.S.* was not a violation of the DMCA,[148] using a valid decryption key identified in a brute force attack only bypasses the permission and not the technological measure. The circumventor's search for the one correct decryption key is analogous to the one password that will allow access. As a result, decryption is probably not a violation of the DMCA under the Permission or TPM Test.

D. REGION CODING

Region coding is usually used in conjunction with encryption in the context of DVDs, but this Section considers region coding in isolation. The circumvention technique analyzed is a region-free DVD player that simply ignores the region bit coded in disks.

1. *Literal Interpretation Test*

Region coding is merely a bit that the copyright holder depends on the player manufacturer to check before a user can play a disc. The copyright owner can refuse to license players that do not check that bit. Similar to *Reimerdes*, where circumventing the encryption on a DVD required the application of a key to decrypt the file, circumventing the region coding requires the application of the region code bit to access the file.[149] Consequently, bypassing this bit probably amounts to a violation of the DMCA under the Literal Interpretation Test.

[147] There are other forms of circumvention that would violate the DMCA under the Permission or TPM Test. For example, in DVDs, player keys are the copyright-holder-sanctioned means of decrypting the movie, but the actual content is encrypted by the title key. If a title key is obtained without using a player key, this would amount to a circumvention under the DMCA. This illustrates the weird result that liability under this test depends not only on what TPM is circumvented, but how it is circumvented. *See generally* The Openlaw DVD/DECSS Forum Frequently Asked Questions (FAQ) List, http://cyber.law.harvard.edu/openlaw/DVD/dvd-discuss-faq.html, *supra* note 94; Matthew Becker & Ahmed Desoky*, supra* note 95.

[148] *See* I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 532–33 (S.D.N.Y. 2004).

[149] *See* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317–19 (S.D.N.Y. 2000), *aff'd*, Universal City Studios, Inc. v. Corely, 273 F.3d 429 (2d Cir. 2001).

2. *Nexus Test*

The first prong of the Nexus Test was analyzed in Section IV.D.I, *supra*, so the only issue remaining is whether the access bears a reasonable relationship to the protections of the Copyright Act. Just like in *MGE* where the copyrighted work could still be copied and accessed, region coding merely prevents initial access but does not encrypt the actual work.[150] The region-coding bit does not protect any copyright holder right because exploiting regional markets is not protected in the Copyright Act.[151] Consequently, there is probably no liability under the Nexus Test.[152]

3. *Other Access Point Test*

Since Region Coding only prevents access by requiring licensed players to check for the region-coding bit, there are many other ways to access the copyrighted work. Without encryption, the region-coding bit does not prevent a user from accessing the work by another means, similar to a user's ability to access the printer code in *Lexmark*. [153] As a result, there is probably no violation of the DMCA under the Other Access Point Test.

4. *Permission or TPM Test*

A user that circumvents the region-coding check by using a region-free player is only circumventing the permission control on the copyrighted work. As the *I.M.S.* court found that the unauthorized user of a valid password only circumvents the permission, the use of an authorized copy in an unauthorized region only circumvents the permission and not any TPM.[154] Consequently, circumventing the region-coding bit is likely not a violation of the DMCA under the Permission or TPM test.

E. ONLINE MOVIE RENTAL PROTECTION

This Section analyzes the circumvention of online movie rental protection by using the clock manipulation trick to extend the length of the allotted movie playback period.

[150] *See* MGE UPS Sys., Inc. v. GE Consumer and Indus., Inc., No. 08-10521, 2010 WL 2820006, *7 (5th Cir. July 20, 2010) *withdrawn* 2010 WL 3769210 (5th Cir. Sept. 29, 2010).

[151] *See* 17 U.S.C. § 106 (2006).

[152] *See* Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1203 (Fed. Cir. 2004).

[153] *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 547 (6th Cir. 2004).

[154] *See* I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 532–33 (S.D.N.Y. 2004).

1. *Literal Interpretation Test*

Since under this legal standard the TPM only needs to effectively control *access* to a copyrighted work,[155] manipulating the movie protection to allow access after the rental should have expired would likely create liability under the DMCA. Here, the MPEG REL is a technological measure that "effectively controls access to a work"[156] because it requires the application of information, the expiration date, to gain access to the work. Just as the *Reimerdes* court found that encryption protection was illegally circumvented to obtain access to the movie,[157] extending the expiration date of a movie rental allows the user to obtain access to the movie longer than legally allowed. The information in this case is illegally modified instead of illegally obtained as it is in *Reimerdes*,[158] but the result is probably the same. Circumventing MPEG REL protection for online movie rentals by extending the rental time is likely a violation of the DMCA under the Literal Interpretation Test.

2. *Nexus Test*

As the first prong of the Nexus Test was analyzed in Section 4.E.2, *supra*, the remaining issue is whether the access bears a reasonable relationship to the protections of the Copyright Act.[159] MPEG REL can be used to prevent copying, but online movie rentals explicitly allow copying for the rental period so the viewer can watch the movie on different devices.[160] Therefore, the access does not bear a reasonable relationship to the protection of the Copyright Act during the correct subscription period. However, after the movie rental expires, the movie is supposed to be deleted from the user's computer and all devices containing copies.[161] After the content is deleted, access of any kind is no longer allowed. The rights of the copyright holder should be protected during that period. Unlike in *Chamberlain* where the copyright holder allowed access to the user indefinitely, extending the rental term exposes the copyright holder to copying and distribution when it should

[155] Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317–19 (S.D.N.Y. 2000), *aff'd*, Universal City Studios, Inc. v. Corely, 273 F.3d 429 (2d Cir. 2001).

[156] 17 U.S.C. § 1201(a)(3)(B).

[157] *See Reimerdes*, 111 F. Supp. 2d at 317–19 .

[158] *See id.*

[159] Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1203 (Fed. Cir. 2004).

[160] *iTunes Store: Movie Rental Frequently Asked Questions*, *supra* note 99.

[161] *Id.*

be disallowed.[162] Therefore, circumvention of MPEG REL probably amounts to a violation of the DMCA.

3. *Other Access Point Test*

Once a movie is rented and downloaded to the viewer's computer, it can be accessed just like any other block of data stored on the user's computer. The MPEG REL TPM does not prevent access through other means during the correct length of the rental. However, once the rental expires, it is supposed to be deleted from the user's computer and any other device it was copied to. As a result, extending the length of the rental period allows access to the file when there should not be any access points. Unlike in *Lexmark* where the approved access to the copyrighted file was indefinite, here, the approved access to the file expires after a limited time.[163] Therefore, circumvention of MPEG REL probably violates the DMCA under the Other Access Point Test.

4. *Permission or TPM Test*

Since the DMCA only "targets the circumvention of digital walls guarding copyrighted material," merely extending the expiration date of a rental movie probably does not violate the Permission or TPM Test.[164] Similar to the *I.M.S.* court's finding that stealing a password only bypasses the permission to access the copyrighted work, changing the expiration date merely extends the permission to access the copyrighted work.[165] Manipulating online movie control protection likely does not create DMCA liability under the Permission or TPM Test.

F. SECRET HANDSHAKES

This Section analyzes the circumvention of the secret handshake using a man-in-the-middle attack as described in Section III.F.

[162] *See* Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1203 (Fed. Cir. 2004).

[163] *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 547 (6th Cir. 2004).

[164] I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 532 (S.D.N.Y. 2004).

[165] *See id.*

1. *Literal Interpretation Test*

Since under this legal standard the TPM only needs to effectively control *access* to a copyrighted work,[166] circumvention using the man-in-the-middle attack will probably violate the DMCA under the Literal Interpretation Test. The challenge-response handshake protocol acts just like password authentication over the Internet. None of the copyrighted data will be streamed to the client until the client correctly responds to the challenge by the server. This is the same basic process as requesting a password from the client, except that the server sends over a random number for the client to calculate the correct "password." The secret handshake is a technological measure that "effectively controls access to a work" because it requires the application of information, the hash value of the server challenge, to gain access to the work.[167] Illegally setting up a secure communication with the server to intercept information is analogous to the activity in *Reimerdes*, in which the court found that the application of an illegally obtained key to access the copyrighted work violated the DMCA.[168] Therefore, circumvention of the secret handshake likely violates the DMCA under the Literal Interpretation Test.

2. *Nexus Test*

The first prong of the Nexus Test was already analyzed in the previous Section IV.F.1. The remaining issue is whether the access method, the secret handshake, bears a reasonable relationship to the protections of the Copyright Act.[169] Since the copyrighted works are all stored across the network, there would be no way to copy or distribute them without circumventing the secret handshake. Whereas in *Chamberlain* the rolling code did not protect the rights of the copyright holder for the locally stored computer program, here, the secret handshake actually protects all access to the remotely stored file so that it cannot be copied or distributed without circumventing the secret handshake.[170] Consequently, circumventing the secret handshake probably violates the DMCA under the Nexus Test.

[166] Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317–19 (S.D.N.Y. 2000), *aff'd*, Universal City Studios, Inc. v. Corely, 273 F.3d 429 (2d Cir. 2001).

[167] *See* 17 U.S.C. § 1201(a)(3)(B) (2006).

[168] *See Reimerdes*, 111 F. Supp. 2d at 317–19.

[169] *See* Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1203 (Fed. Cir. 2004).

[170] *See id.* at 1203–04.

3. *Other Access Point Test*

Since the copyrighted works are all stored remotely, there are no other access points to the copyrighted works without circumventing the secret handshake. Unlike in *Lexmark*, where the user had access to the copyrighted works on the printer, here, access is only permitted through a secure connection with the remote server that must be set up using the secret handshake.[171] As a result, circumventing the secret handshake probably violates the DMCA under the Other Access Point Test as well.

4. *Permission or TPM Test*

Similar to the use of an illegally obtained password in *I.M.S.*, using the man-in-the-middle attack to illegally obtain a correct response to the server challenge circumvents the "permission to engage and move through the technological measure."[172] However, it does not circumvent the "digital walls guarding copyrighted material," which are recognized under the DMCA.[173] Therefore, circumvention of the secret handshake likely does not violate the DMCA using the Permission or TPM test.

G. WATERMARKING AND ACP

This Section analyzes liability under the DMCA for removing the watermark data from a copy and digitizing an analog copy of a work with ACP to circumvent the protection.[174]

1. *Literal Interpretation Test*

Under this legal standard, the TPM only needs to effectively control *access* to a copyrighted work.[175] However, neither watermarks nor ACP actually control access to the copyrighted work. Any copyrighted work with a digital watermark can still be accessed freely.[176] And ACP merely adds data to the copyrighted work so any copy made by an analog recording device will be

[171] *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 547 (6th Cir. 2004).

[172] *See* I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 532 (S.D.N.Y. 2004).

[173] *See id.*

[174] Note that although this Section finds it unlikely that circumventing these protection measures violates the DMCA, it is still not unreasonable that circumvention may trigger DMCA suits. *See* JT Smith, *supra* note 118.

[175] Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317–19 (S.D.N.Y. 2000), *aff'd*, Universal City Studios, Inc. v. Corely, 273 F.3d 429 (2d Cir. 2001).

[176] Maurice Maes et al., *Digital Watermarking DVD Video Copy Protection: What Issues Play a Role in Designing an Effective System?*, IEEE Signal Processing Magazine (2000) at 2–4.

unwatchable.[177] Unlike the encryption scheme in *Reimerdes*, use of ACP or watermarking protection does not change the accessibility of all of the bits representing the copyrighted work.[178] Therefore, under the Literal Interpretation Test, circumventing watermarking or ACP probably does not constitute a violation of the DMCA because neither means of protection prevents access.

2. *Nexus Test*

Since access is not controlled by watermarking and ACP, circumvention is probably not a violation of the DMCA under the Nexus Test.[179]

3. *Other Access Point Test*

Similarly, as works utilizing watermarking and ACP are freely accessible from any access point, circumventing these measures likely does not violate the DMCA under the Other Access Point Test.[180]

4. *Permission or TPM Test*

Since watermarking and ACP do not need to be circumvented to gain access to the entire work, it is irrelevant whether the TPM or permission was actually circumvented.[181] Therefore, there is probably no violation under the Permission or TPM Test.[182]

A summary of the legal classifications for each TPM under the four legal standards is found in Table 2.

[177] Eskicioglu & Delp, *supra* note 114, at 682.

[178] *See Reimerdes*, 111 F. Supp. 2d at 317–19.

[179] *See* Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1203–04 (Fed. Cir. 2004).

[180] *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 547 (6th Cir. 2004).

[181] *See* I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 532 (S.D.N.Y. 2004).

[182] Even though circumventing watermarking and ACP is likely not a circumvention under § 1201, § 1202 imposes liability for altering or removing "any copyright management information." 17 U.S.C. § 1202(b)(1) (2006). Removing a watermark may be a violation under § 1202.

Table 2: Summary of TPMs Classified by Legal Standard

		Legal Standards			
		Literal Interpretation Test	**Nexus Test**	**Other Access Point Test**	**Permission or TPM Test**
TPMs	**Password Protection**	Very likely violation	Likely violation if work is stored remotely	Likely violation if work is stored remotely	S.D.N.Y. held no violation[183]
	Dongles	Very likely violation	5th Circuit withdrawn decision found no violation[184]	Very likely no violation	Likely violation
	Encryption	2nd Circuit affirmed violation[185]	Possible violation	Likely violation	Likely no violation
	Region Coding	Very likely violation	Likely no violation	Likely no violation	Likely no violation
	Online Movie Protection	Very likely violation	Very likely violation	Very likely violation	Likely no violation
	Secret Handshakes	Very likely violation	Likely violation	Likely violation	Likely no violation
	Watermarking and ACP	Very likely no violation	Very likely no violation	Very likely no violation	Very likely no violation

V. CONCLUSION

The exact legal standard that should be applied in anti-circumvention DMCA cases is still under debate. This Note provides a framework to show how some of the most common TPMs fit (or do not fit) the various legal tests used by courts. Further, this Note offers some guidance as to which TPMs can be clearly circumvented without violating the DMCA.

[183] *I.M.S.*, 307 F. Supp. 2d at 532 (S.D.N.Y. 2004).

[184] MGE, No. 08-10521, 2010 WL 2820006, *3 (5th Cir. July 20, 2010) *withdrawn* 2010 WL 3769210 (5th Cir. Sept. 29, 2010).

[185] *See* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317–19 (S.D.N.Y. 2000), *aff'd*, Universal City Studios, Inc. v. Corely, 273 F.3d 429 (2d Cir. 2001).

Although the Literal Interpretation Test has been used in most anti-circumvention DMCA cases, it may not be the best test. While it does follow the plain language of the statute,[186] the result of the test does not always align with legislative intent.[187] The Electronic Frontier Foundation (EFF) is one of the most outspoken critics of an overly broad interpretation of the DMCA because it could stifle free speech, prevent competition, and threaten legitimate scientific research.[188] Courts have modified the Literal Interpretation Test where the copyright holder asserted a DMCA claim for improper purposes,[189] but such modification can cause higher burdens for legitimate anti-circumvention claims.[190]

The Nexus Test, the Other Access Point Test, and the Permission or TPM Test described in this Note all seem ill-suited to cover all anti-circumvention claims because of the inconsistencies and ambiguities discussed in Part IV, *supra*.[191] The Federal Circuit even recognized that "such a rule of reason may create some uncertainty and consume some judicial resources."[192]

The ideal test for determining whether the circumvention of a TPM constitutes a violation of the DMCA should consider the purpose for which the DMCA claim is being brought. Allowing DMCA claims to reinforce a monopoly would go against the legislative intent because "Congress did not intend to allow the DMCA to be used offensively [to create monopolies], but rather only sought to reach those who circumvented protective measures 'for

[186] *See* 17 U.S.C. § 1201; NIMMER, *supra* note 28, at § 12A.03.

[187] *See* 17 U.S.C. § 1201; 17 U.S.C. § 1201; *see also* 144 Cong. Rec. H7093, H7094-95 (Aug. 4, 1998); S. REP. NO. 105-90, at 29 (1998); H.R. REP. NO. 105-551, pt. 1, at 18 (1998); H.R. REP. NO. 105-551, pt. 2, at 38 (1998). *Cf.* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 546 (6th Cir. 2004) (trying to prevent compatibility of third party printer ink cartridges); Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1204 (Fed. Cir. 2004) (trying to prevent compatibility of third party garage door openers); Davidson & Assocs. v. Jung, 422 F.3d 630 (8th Cir. 2005) (trying to prevent compatibility of third party game servers).

[188] *See* Fred Von Lohmann, *Unintended Consequences: 12 Years Under the DMCA*, 1–2 (2010).

[189] *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004); *Chamberlain*, 381 F.3d 1178 (Fed. Cir. 2004).

[190] *See* MGE I, No. 08-10521, 2010 WL 2820006 (2010).

[191] *See* discussion *supra* Section IV.A (discussing different results depending how the TPM is circumvented); *supra* Section IV.C.2 (discussing different results depending on if a copy of an encrypted work is a copy under the Copyright Act); *supra* Section IV.C.4 n. 147 (discussing different results depending on specific technical details of the encryption used); *supra* Section IV.G n. 174 (discussing potential DMCA liability even though access to the copyrighted work is not prevented by watermarking and ACP).

[192] *Chamberlain*, 381 F.3d at 1202–03.

the purpose' of pirating works protected by the copyright statute."[193] For example, in *Lexmark,* where the DMCA claim was brought against a third party ink cartridge manufacturer to prevent competition, this purpose factor would weigh heavily against the copyright holder.[194] Conversely, in *Reimerdes*, where the copyright holder was trying to prevent his movies from being illegally copied, the purpose factor would weigh heavily in favor of the copyright holder.[195] Admittedly, adding a subjective component to any test potentially poses the problem of judicial discretion and inconsistent opinions. However, without a purpose factor, the DMCA may be used to prevent competition when it is interpreted too broadly[196] or it may ignore a valid circumvention claim when it is interpreted too narrowly.[197]

APPENDIX I: TECHNICAL DEFINITIONS

Brute Force refers to a method of finding an unknown password or key by trial and error. Typically, a hacker will try every possible password or key until the correct one is found.[198]

Copying in the digital technology field is simply the process of replicating the data stored in one location in another location.[199] Since all data is represented by a string of ones and zeroes, copying is just replicating that string of digits.

Hacking is the process of modifying the code of a program to change the way the program functions.[200] For circumvention purposes, a program's code can be changed to no longer ask for a CD key, check for a dongle, or prompt the user for a password.

[193] *Lexmark*, 387 F.3d at 552 (Merritt, C.J., concurring).

[194] *See id.*

[195] *See* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 308–15 (S.D.N.Y. 2000).

[196] *See, e.g.*, Davidson & Assocs. v. Jung, 422 F.3d 630, 633 (8th Cir. 2005) (construing the DMCA broadly to prevent competition to the copyright holder from a third party game server).

[197] *See, e.g.*, MGE I, No. 08-10521, 2010 WL 2820006, *3 (2010) (construing the DMCA narrowly based on the *Chamberlain* Nexus Test such that there is no liability for circumvention of a dongle protecting the plaintiff's copyrighted software).

[198] *Brute Force Definition*, DICTIONARY.COM, http://dictionary.reference.com/browse/brute+force (last visited Nov. 19, 2010).

[199] BISHOP, *supra* note 74, at 860–61.

[200] Robert J. Sciglimpiaglia, Jr., *Computer Hacking: A Global Offense*, 3 PACE INT'L L. REV. 1, 199 (1991).

Hash is a function that converts a bit string of any length into a single integer in an array.[201] Hashes are often used to verify that a bit string is correct or that it has not been changed. A hash function must be a one-way function, such that it is easy to compute the hash, but very hard to reverse the function to determine the original bit string from the hash.[202]

Encryption involves encoding the copyrighted work in such a way that it is a meaningless string of bits.[203] Unlocking the encryption requires a key, which is a predefined number that is used to decrypt the copyrighted work.[204]

[201] WEISS, *supra* note 90, at 181–84.

[202] ALFRED J. MENEZES, PAUL C. VAN OORSCHOT, & SCOTT A. VANSTONE, HANDBOOK OF APPLIED CRYPTOGRAPHY 8 (1997).

[203] BISHOP, *supra* note 74, at 217–18.

[204] *Id.*