V.

Digital Millennium Copyright Act— 17 U.S.C. §§ 1201-1205

V.A. Introduction

V.A.1. DMCA's Background and Purpose

With the advent of digital media and the Internet as a means to distribute such media, large-scale digital copying and distribution of copyrighted material became easy and inexpensive. In response to this development, and to prevent large-scale piracy of digital content over the Internet, in 1997 the World Intellectual Property Organization (WIPO) responded with two treaties, the Copyright Treaty, and the Performances and Phonograms Treaty, to prohibit pirates from defeating the digital locks that copyright owners use to protect their digital content from unauthorized access or copying. Specifically, Article 11 of the WIPO Copyright Treaty prescribes that contracting states

> shall 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 restricts acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.

See WIPO Copyright Treaty, Apr. 12, 1997, S. Treaty Doc. No. 105-17, art. 11 (1997); WIPO Performances and Phonograms Treaty, Apr. 12, 1997, S. Treaty Doc. No. 105-17, art. 18 (1997) (same with respect to performers or producers of phonograms). The United States signed these treaties on April 12, 1997, and ratified them on October 21, 1998. *See* 144 Cong. Rec. 27,708 (1998) (Resolution of Ratification of Treaties).

To implement these treaties, Congress enacted Title I of the Digital Millennium Copyright Act (DMCA) on October 28, 1998, with the twin goals of protecting copyrighted works from piracy and promoting electronic commerce. *See* H.R. Rep. No. 105-551 (II), at 23 (1998); S. Rep. No. 105-190, at 8 (1998); *see also Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 454 (2d Cir. 2001); *United States v. Elcom, Ltd.*, 203 F. Supp. 2d 1111, 1129-30 (N.D. Cal. 2002). Congress accomplished these goals by enacting prohibitions relating to the circumvention of copyright protection systems as set forth in 17 U.S.C. § 1201, and the integrity of copyright management information pursuant to 17 U.S.C. § 1202.

Criminal enforcement has largely focused on violations of the anti-circumvention and anti-trafficking prohibitions in 17 U.S.C. § 1201, and thus these are the main focus of this chapter. For a more complete discussion of the provisions that protect the integrity of copyright management information, as set forth in 17 U.S.C. § 1202, see Section V.B.5. of this Chapter.

V.A.2. Key Concepts: Access Controls vs. Copy Controls, Circumvention vs. Trafficking

Section 1201 contains three prohibitions. First, it prohibits "circumvent[ing] a technological measure that effectively controls access to a work protected under this [copyright] title." 17 U.S.C. § 1201(a)(1)(A). Second, it prohibits the manufacture of or trafficking in products or technology designed to circumvent a technological measure that controls access to a copyrighted work. 17 U.S.C. § 1201(a)(2). Third, it prohibits the manufacture of or trafficking in products or technology designed to circumvent measures that protect a copyright owner's rights under the Copyright Act. 17 U.S.C. § 1201(b). As noted more fully in Section V.C. of this Chapter, the DMCA provides several exceptions.

Title I of the DMCA creates a separate private right of action on behalf of "[a]ny person injured by a violation of section 1201 or 1202" in federal district court. 17 U.S.C. § 1203(a). These prohibitions are criminally enforceable against any person who violates them "willfully and for purposes of commercial advantage or private financial gain," excluding nonprofit libraries, archives, educational institutions, and public broadcasting entities as defined by 17 U.S.C. § 118(f). 17 U.S.C. § 1204(a), (b). (At this writing, the reference to § 118(g) at § 1204(b) has not been amended to indicate the provision's current location at § 118(f).)

Although civil actions do not require the claimant to establish that a DMCA violation was "willful" or for "commercial advantage or private financial gain," the substantive law defining violations of §§ 1201 or 1202 is generally the same for both criminal and civil actions. Thus, published decisions relating to whether a violation of these DMCA sections has occurred in civil cases are instructive in criminal cases.

V.A.2.a. Access Controls vs. Copy/Use Controls

To understand the technical requirements of the DMCA's criminal prohibitions, it is first important to understand what technology the DMCA generally applies to, and what the DMCA outlaws. Congress intended Title I of the DMCA to apply to copyrighted works that are in *digital* format and thus could easily and inexpensively be accessed, reproduced, and distributed over the Internet without the copyright owner's authorization. The DMCA therefore applies to what one might call a "digital lock"—a technological measure that copyright owners use to control who may see, hear, or use copyrighted works stored in digital form. These digital locks are commonly called either "access controls" or "copy controls," depending on what function the digital lock is designed to control.

The DMCA states that a digital lock, or "technological measure" (as the DMCA refers to such locks), constitutes an *access control* "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." 17 U.S.C. § 1201(a)(3)(B). Thus, as the name suggests, an access control prevents users from accessing a copyrighted work without the author's permission. For example, a technology that permits access to a newspaper article on an Internet Web site only by those who pay a fee or have a password would be considered an access control. *See* S. Rep. No. 105-190, at 11-12 (1998). In this example, the author (i.e., copyright owner) uses such fees or password requirements as access controls that allow the author to distinguish between those who have the author's permission to read the online article from those who do not. If a user does not pay the fee or enter the password, then the user cannot lawfully read the article or otherwise access it.

The DMCA also prescribes that a digital lock constitutes a *copy control* "if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title." 17 U.S.C. § 1201(b)(2)(B). The rights of a copyright owner include the exclusive rights to reproduce the copyrighted work, to prepare derivative works based upon the copyrighted work, to distribute copies by sale or otherwise, to perform the copyrighted work publicly, and to display the copyrighted work publicly. 17 U.S.C. § 106. In other words, such a digital lock prevents someone from making an infringing use of a copyrighted work *after* the user has already accessed the work. *See* S. Rep. No. 105-190, at 11-12 (1998); *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 441 (2d Cir. 2001). Although some courts will refer to such digital locks as "usage controls" because such locks conceivably seek to control all infringing uses, in practice, these digital locks typically control unauthorized copying of the work—hence the name "copy control."

To illustrate an example of a copy control, consider again the online newspaper article referenced above. A technological measure on an Internet Web site that permits a user to read (i.e., access) the online article but prevents the viewer from making a copy of the article once it is accessed would be a copy control. *See* S. Rep. No. 105-190, at 11-12 (1998). Thus, access and copy controls are different kinds of digital locks that are each designed to perform different functions. Whereas an access control blocks *access* to the copyrighted work—such as a device that permits access to an article on an Internet Web site only by those who pay a fee or have a password—a copy control protects the copyright itself—such as a device on the same Web site that prevents the viewer from copying the article once it is accessed.

Although the DMCA's distinction between an "access control" and a "copy control" appears straightforward in principle, courts are not always consistent in how they characterize a particular protection technology. For example, in the 1990s, the DVD industry developed the Content Scramble System (CSS)—an encryption scheme incorporated into DVDs that employs an algorithm configured by a set of "keys" to encrypt a DVD's contents. For a DVD player to display a movie on a DVD encoded with CSS, the DVD player must have the "player keys" and the algorithm from the copyright owner. The Second Circuit characterized this CSS technology as an "access control" because a DVD player with the proper player keys and algorithm from the copyright owner "can display the movie on a television or a computer screen, but does not give a viewer the ability to use the copy function of the computer to copy the movie or to manipulate the digital content." *Corley*, 273 F.3d at 437. A district court in the Northern District of California, however, viewed the same technology as both an access control and a copy control. *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1095 (N.D. Cal. 2004). Accordingly, prosecutors should be careful how they characterize technological controls as access or copy controls, and in some instances it may even be advisable for prosecutors to characterize a particular copyright protection system as both.

V.A.2.b. Circumvention vs. Trafficking in Circumvention Tools

Section 1201(a) of the DMCA proscribes two kinds of conduct regarding *access controls*: 1) circumvention of access controls, 17 U.S.C. § 1201(a)(1), and 2) trafficking in technology primarily designed to facilitate circumvention of access controls, 17 U.S.C. § 1201(a)(2). Both of these prohibitions relating to access controls are discussed more fully in Sections V.B.1. and V.B.2. of this Chapter.

Unlike § 1201(a), however, Congress did not ban the act of circumventing *copy controls*. Instead, § 1201(b) only prohibits trafficking in technology primarily designed to facilitate the circumvention of copy controls. 17 U.S.C. § 1201(b)(1). Congress expressly chose not to prohibit the circumvention of copy controls in the DMCA because circumventing a copy control is essentially an act of copyright infringement that is already covered by copyright law. S. Rep. No. 105-190, at 12 (1998).

Thus, § 1201(a)(1) (the "anti-circumvention provision") prohibits the actual *use* of circumvention technology to obtain access to a copyrighted work without the copyright owner's authority. In contrast, §§ 1201(a)(2) and 1201(b)(1) (the "anti-trafficking provisions") focus on the *trafficking* in circumvention technology, regardless of whether such technology ultimately leads a third party to circumvent an access or copy control. *See Davidson & Assocs. v. Jung*, 422 F.3d 630, 640 (8th Cir. 2005); *Corley*, 273 F.3d at 440-41. And with respect to the anti-trafficking provisions, "although both sections prohibit trafficking in a circumvention technology, the focus of § 1201(a)(2) is circumvention of technologies designed to *prevent access* to a work, and the focus of § 1201(b)(1) is circumvention of technologies designed to *permit access* to a work but *prevent copying* of the work or some other act that infringes a copyright." *Davidson*, 422 F.3d at 640 (emphasis in original).

The following chart illustrates the distinction:

	Access	Copy
Circumventing	§ 1201(a)(1)	No DMCA violation, but potential copyright violation: 17 U.S.C. § 506; 18 U.S.C. § 2319
Trafficking	§ 1201(a)(2)	§ 1201(b)(1)

V.A.3. Differences Between the DMCA and Traditional Copyright Law

Whereas copyright law focuses on "direct" infringement of a copyrighted work, the DMCA focuses largely on the facilitation of infringement through circumvention tools and services primarily designed or produced to circumvent an access or copy control. In other words, the DMCA represents a shift in focus from infringement to the tools of infringers.

Before the DMCA was enacted, copyright law had only a limited application to the manufacture or trafficking of tools designed to facilitate copyright infringement. In 1984, the Supreme Court held that "the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses." *Sony v. Universal City Studios*, 464 U.S. 417, 442 (1984). Under this standard, a copy control circumvention tool would not violate copyright law if it were "widely used for legitimate ... purposes" or were merely "capable of substantial noninfringing uses." *Id.*

The DMCA shifts the focus from determining whether the downstream use of equipment will be used for infringement, to determining whether it was primarily designed to circumvent an access or copy control—even if such equipment were ultimately capable of substantial noninfringing uses. *See* 17 U.S.C. § 1201(a)(2)(A), (b)(1)(A). For example, with respect to software primarily designed to circumvent copy controls on DVDs, courts have held "that legal downstream use of the copyrighted material by customers is not a defense to the software manufacturer's violation of the provisions of § 1201(b)(1)." *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1097-98 (N.D. Cal. 2004). Thus, although trafficking in circumvention technology that is capable of substantial noninfringing uses may not constitute copyright infringement, it may still violate the DMCA if such technology is primarily designed to circumvent access or copy controls. *See RealNetworks, Inc. v. Streambox, Inc.*, No. 2:99CV02070, 2000 WL 127311, at *7 (W.D. Wash. Jan. 18, 2000).

The DMCA also added a new prohibition against circumventing access controls, even if such circumvention does not constitute copyright infringement. 17 U.S.C. § 1201(a)(1)(A). Prior to the DMCA, "the conduct of circumvention [of access controls] was never before made unlawful." S. Rep. No. 105-190, at 12 (1998); *cf. Chamberlain Group, Inc. v. Skylink Techs.,* *Inc.*, 381 F.3d 1178, 1195-96 (Fed. Cir. 2004). By the same token, the DMCA does not contain a parallel prohibition against the use—infringing or otherwise—of copyrighted works once a user has access to the work. *United States v. Elcom*, 203 F. Supp. 2d 1111, 1121 (N.D. Cal. 2002) (holding that "circumventing use restrictions is not unlawful" under the DMCA); *cf.* S. Rep. No. 105-190, at 12 (1998) ("The copyright law has long forbidden copyright infringements, so no new prohibition was necessary.").

Although the DMCA "targets the *circumvention* of digital walls guarding copyrighted material (and trafficking in circumvention tools), [it] does not concern itself with the *use* of those materials after circumvention has occurred." *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 443 (2d Cir. 2001); *cf. 321 Studios*, 307 F. Supp. 2d at 1097 (holding that "the downstream uses of the [circumvention] software by the customers of 321 [the manufacturer], whether legal or illegal, are not relevant to determining whether 321 itself is violating [the DMCA]"). At the same time, the DMCA also cautions that "[n]othing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title." 17 U.S.C. § 1201(c)(1); *Elcom*, 203 F. Supp. 2d at 1120 ("Congress did *not* ban the act of circumventing the use restrictions ... because it sought to preserve the fair use rights of persons who had lawfully acquired a work"). Thus, a criminal defendant who has violated the DMCA by circumventing an access control has not necessarily infringed a copyrighted work under copyright law. Accordingly, prosecutors must apply traditional copyright law instead of the DMCA to prosecute infringing uses of copyrighted works, including the circumvention of copy controls. By the same token, to demonstrate a violation of the DMCA, prosecutors need not establish copyright infringement, nor even an intent to infringe copyrights.

In addition, unlike in a civil copyright claim, a victim's failure to register its copyrighted work is not a bar to a DMCA action. See Section V.B.1.c. of this Chapter.

V.A.4. Other DMCA Sections That Do Not Concern Prosecutors

Of the DMCA's five titles, the only one that need concern prosecutors is Title I, which was codified at 17 U.S.C. §§ 1201-1205. The remaining four titles concern neither criminal prosecutions nor those provisions of the WIPO treaties that the DMCA was originally designed to implement. Title II concerns the liability of Internet service providers for copyright infringement over their networks. It amended the copyright code by enacting a new § 512, which gives Internet service providers some immunity in return for certain business practices, and requires them to obey certain civil subpoenas to identify subscribers alleged to have committed infringement. Section 512 does not, however, authorize criminal subpoenas for the same purpose.

Title III of the DMCA clarifies that a lawful owner or lessee of a computer may authorize an unaffiliated service provider to activate the computer to service its hardware components. Title IV of the DMCA mandates a study of distance learning; permits libraries and archives to use the latest technology to preserve deteriorating manuscripts and other works; and permits transmitting organizations to engage in ephemeral reproductions, even if they need to violate the newly-added anti-circumvention features in the process. Finally, Title V of the DMCA extends the scope of the Copyright Act's protection to boat hulls.

For purposes of this manual, all references to the DMCA concern Title I unless the context demands otherwise.

V.B. Elements of the Anti-Circumvention and Anti-Trafficking Provisions

V.B.1. Circumventing Access Controls—17 U.S.C. §§ 1201(a)(1) and 1204

The DMCA prohibits "circumvent[ing] a technological measure that effectively controls access to a work protected under this [copyright] title." 17 U.S.C. § 1201(a)(1)(A). To prove a violation of 17 U.S.C. §§ 1201(a)(1) and 1204, the government must establish that the defendant

1. willfully
2. circumvented
3. a technological measure that effectively controls access (i.e., an access control)
4. to a copyrighted work
5. for commercial advantage or private financial gain.

For purposes of the DMCA, prosecutors may look to the law of copyright infringement for guidance regarding the "willfully" element and the "commercial advantage" element. See Chapter II of this Manual.

Two recent cases from the Federal Circuit have read an additional element into § 1201(a) offenses, holding that the unauthorized access must also infringe or facilitate infringing a right protected by the Copyright Act to establish violations of 17 U.S.C. § 1201(a)(1) and (a)(2). *Storage Technology Corp. v. Custom Hardware Eng'g & Consulting, Inc.* ("*StorageTek*"), 421 F.3d 1307, 1318 (Fed. Cir. 2005) (quoting *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178, 1203 (Fed. Cir. 2004)). Although the results in *Chamberlain* and *StorageTek* are consistent with Congress's intent that § 1201(a) apply to measures controlling access to copyrighted works in digital form (see Section V.B.1.d. of this Chapter), the courts reached those results using a flawed analysis. Neither the DMCA's plain language nor its legislative history permits circumvention of access controls or trafficking in access or copy control circumvention devices to enable a fair use, as opposed to an infringing use. The government has consistently argued that the DMCA prohibits the manufacture and trafficking in *all* circumvention tools, even those designed to facilitate fair use. See Section V.C.10.d. of this Chapter. Additionally, unlike the regional circuits, the Federal Circuit does not have the authority to develop a body of case law on copyright law that is independent of the regional circuits. *StorageTek*, 421 F.3d at 1311; *Chamberlain*, 381 F.3d at 1181. Accordingly, until a regional circuit adopts the *StorageTek-Chamberlain* position regarding the additional element to a § 1201(a) offense, prosecutors should oppose any attempts to cite these decisions as meaningful precedent. If a defendant does attempt to rely on these decisions, prosecutors are encouraged to contact CCIPS at (202) 514-1026 for sample briefs and other guidance to oppose them.

V.B.1.a. Circumventing

To "circumvent" an access control "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." 17 U.S.C. § 1201(a)(3)(A). Thus, to establish this element, the government first must prove that the defendant 1) *bypassed* a technological measure, and 2) did so *without the authority of the copyright owner*.

"Circumvention requires either descrambling, decrypting, avoiding, bypassing, removing, deactivating or impairing a technological measure *qua* technological measure." *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*, 401 F. Supp. 2d 105, 113 (D.D.C. 2005) (same); *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 443 (2d Cir. 2001). In other words, circumvention of an access control occurs when someone bypasses the technological measure's gatekeeping capacity, thereby precluding the copyright owner from determining which users have permission to access the digital copyrighted work and which do not. *I.M.S.*, 307 F. Supp. 2d at 532.

For example, in *Corley*, the Second Circuit characterized CSS, the scheme for encrypting digital movies stored on DVDs, as an access control similar to "a lock on a homeowner's door, a combination of a safe, or a security device attached to a store's products." *Corley*, 273 F.3d at 452-53. A licensed DVD player would be, in this metaphor, the homeowner's key to the door. *Id.* The court held that defendant's computer program, called "DeCSS," circumvented CSS because it decrypted the CSS algorithm to enable "anyone to gain access to a DVD movie without using a [licensed] DVD player." *Id.* at 453. DeCSS functions "like a skeleton key that can open a locked door, a combination that can open a safe, or a device that can neutralize a security device attached to a store's products." *Id.* Thus, using DeCSS to play a DVD on an unlicensed player circumvents an access control because it undermines the copyright owner's ability to control who can access the DVD movie. *Id.*

Circumvention does not occur, however, by properly *using* the technological measure's gatekeeping capacity without the copyright owner's permission. *Egilman*, 401 F. Supp. 2d at 113 (holding that the definition of circumvention is missing "any reference to 'use' of a technological measure without the authority of the copyright owner"); *see also I.M.S.*, 307 F. Supp. 2d at 533 ("Whatever the impropriety of defendant's conduct, the DMCA and the anti-circumvention provision at issue do not target this sort of activity."). Using CSS as an example, a defendant does not circumvent a DVD's access control, CSS, by merely borrowing another person's licensed DVD player to view the DVD, even if the defendant did not receive permission from the owner of the licensed DVD player to "borrow" the player. No circumvention has occurred because the defendant would not have bypassed CSS. In fact, he would have viewed the DVD exactly as the copyright owner had intended—by using a licensed DVD player. Courts have similarly held that a defendant who without authorization uses a valid password to access a password-protected website containing copyrighted works does not engage in circumvention because the defendant used an authorized password rather than disabled the access control (here, the password protection mechanism). *See Egilman*, 401 F. Supp. 2d at 113-14; *I.M.S.*, 307 F. Supp. 2d at 531-33. In this example, other charges might be available if the defendant obtained information from a protected computer. *I.M.S.*, 307 F. Supp. 2d at 524-26 (discussing possible violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)).

In addition, for there to be a circumvention pursuant to § 1201(a)(3)(A), the circumvention must occur "without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A). A defendant who decrypts or avoids an access control measure with the copyright owner's authority has not committed a "circumvention" within the meaning of the statute.

The fact that a purchaser has the right to use a purchased product does not mean that the copyright owner has authorized the purchaser to circumvent the product's access controls. For instance, a purchaser of a CSS-encrypted DVD movie clearly has the "authority of the copyright owner" to view the DVD but does not necessarily have the authority to view it on *any* platform capable of decrypting the DVD. *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1096 (N.D. Cal. 2004) (holding "that the purchase of a DVD does not give to the purchaser the authority of the copyright holder to decrypt CSS"). *See also Davidson & Assocs. v. Jung*, 422 F.3d 630, 641 (8th Cir. 2005) (holding that purchasers of interactive gaming software had permission to use the game but lacked the copyright owner's permission to circumvent the encryption measure controlling access to the game's interactive mode). Thus, purchasers of products containing copyrighted works—by virtue of that purchase alone—do not necessarily have the copyright owner's permission to circumvent a technological measure controlling access to the copyrighted work.

V.B.1.b. Technological Measures That Effectively Control Access ("Access Control")

As already noted, 17 U.S.C. § 1201(a) concerns technological measures designed to prevent *access* to a copyrighted work—technology typically referred to as "access controls." A technological measure does not constitute an access control under the DMCA unless it "effectively controls access to a work." 17 U.S.C. § 1201(a)(1)(A). "[A] technological measure 'effectively controls access to a [copyrighted] 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." 17 U.S.C. § 1201(a)(3)(B).

An access control "effectively controls access to a work" if its ordinary function and operation is to control access to a copyrighted work's expression, regardless of whether or not the control is a strong means of protection. *See*, *e.g.*, *321 Studios*, 307 F. Supp. 2d at 1095.

Significantly, courts have rejected the argument that the meaning of the term "effectively" is based on how successful the technological measure is in controlling access to a copyrighted work. *See*, *e.g.*, *id.* (holding that the fact that the CSS decryption keys permitting access to DVDs were "widely available on the internet [sic]" did not affect whether CSS was "effective" under the DMCA). For example, protection "measures based on encryption or scrambling 'effectively control' access to copyrighted works, although it is well known that what may be encrypted or scrambled often may be decrypted or unscrambled." *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 318 (S.D.N.Y. 2000) (footnote omitted), *aff'd sub nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001). Equating "effectively" with "successfully" "would limit the application of the statute to access control measures that thwart circumvention, but withhold protection for those measures that can be circumvented" and consequently "offer protection where none is needed" while "withhold[ing] protection precisely where protection is essential." *Id*; *see also Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 549 (6th Cir. 2004) ("A precondition for DMCA liability is not the creation of an impervious shield to the copyrighted work .... Otherwise, the DMCA would apply only when it is not needed.") (internal citations omitted).

Although the DMCA does not define "access," at least one court has held that controlling access to a copyrighted work means controlling access to the expression (e.g., controlling the ability to see or to read the actual text of a copyrighted computer program, hear a copyrighted song, or watch a copyrighted movie) contained in a copyrighted work. *Lexmark*, 387 F.3d at 547 (holding that an authentication sequence that prevented "access" to a copyrighted computer program on a printer cartridge chip by preventing the printer from functioning and the program from executing did not "control[] access" under the DMCA because the copyrighted work's expression (the computer program) was nonetheless "freely readable"). In the context of a computer program, the Sixth Circuit held that an access control under the DMCA must control access to the program's copyrighted expression—i.e., control the ability to see or to read the program's code. *Id.* at 548. On the other hand, a technological measure that controls only the function of a copyrighted computer program but leaves the code freely readable is not an access control under the DMCA. *Compare id.* (holding that there is no precedent deeming a control measure as one that "effectively controls access" under the DMCA "where the [purported] access-control measure left the literal code or text of the computer program or data freely readable") *with Agfa Monotype Corp. v. Adobe Sys., Inc.*, 404 F. Supp. 2d 1030, 1036 (N.D. Ill. 2005) (holding that font embedding bits are not technological measures that "effectively control access" because they "have been available for free download from the Internet" and are "not secret or undisclosed. Embedding bits are not encrypted, scrambled or authenticated, and software applications ... need not enter a password or authorization sequence to obtain access to the embedding bits or the specification for the" font), *and Davidson*, 422 F.3d at 641 (holding that a technological measure that controlled access to a computer program's expression that otherwise "was not freely available" "without acts of reverse engineering" constituted an "access control" under the DMCA).

V.B.1.c. To a Copyrighted Work

The access control also must have controlled access to a copyrighted work. *See* 17 U.S.C. § 1201(a)(1)(A), (2)(A)-(C) (referring repeatedly to "a work protected under this title [17]"). The protection of a copyrighted work is an essential element. *See* S. Rep. No. 105-190, at 28-29 (1998). The DMCA's anti-circumvention prohibition does not apply to someone who circumvents access controls to a work in the public domain, like a book of Shakespeare, because such a protection measure controls access to a work that is not copyrighted. *Cf. United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1131-32 (N.D. Cal. 2002).

A victim's failure to register its copyrighted work is not a bar to a DMCA action. *See I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.*, 307 F. Supp. 2d 521, 531 n.9 (S.D.N.Y. 2004); *Medical Broad. Co. v. Flaiz*, No. Civ.A. 02-8554, 2003 WL 22838094, at *3 (E.D. Pa. Nov. 25, 2003) (finding that "[w]hile a copyright registration is a prerequisite under 17 U.S.C. § 411(a) for an action for [civil] copyright infringement, claims under the DMCA ... are simply not copyright infringement claims and are separate and distinct from the latter") (citation omitted).

V.B.1.d. How Congress Intended the Anti-Circumvention Prohibition to Apply

Courts have acknowledged that, on its face, § 1201(a)(1) prescribes that one unlawfully circumvents an access control even where the ultimate goal of such circumvention is fair use of a copyrighted work. *See, e.g., Reimerdes*, 111 F. Supp. 2d at 304 (holding that an unlawful circumvention of a technological measure can occur even though "[t]echnological access control measures have the capacity to prevent fair uses of copyrighted works as well as foul"). Although Congress was concerned that the DMCA's anti-circumvention prohibition could be applied to prevent circumvention of access controls for legitimate fair uses, Congress concluded that strong restrictions on circumvention of access control measures were essential to encourage digital works because otherwise such works could be pirated and distributed over the Internet too easily. *See Lexmark*, 387 F.3d at 549.

For this reason, courts will strictly apply § 1201(a) to copyrighted expression stored in a digital format whereby, for instance, executing encrypted computer code containing the copyrighted expression actually generates the visual and audio manifestation of protected expression. *Lexmark*, 387 F.3d at 548 (holding that Congress intended § 1201(a) to apply where executing "encoded data on CDs translates into music and on DVDs into motion pictures, while the program commands in software for video games or computers translate into some other visual and audio manifestation"); *see also 321 Studios*, 307 F. Supp. 2d at 1095 (movies on DVDs protected by an encryption algorithm (CSS) cannot be watched without a DVD player that contains an access key decrypting CSS); *Davidson*, 422 F.3d at 641 (encrypted algorithm on computer game prevented unauthorized interactive use of computer game online); *Pearl Inv., LLC v. Standard I/O, Inc.*, 257 F. Supp. 2d 326, 349 (D. Me. 2003) ("encrypted, password-protected virtual private network" prevented unauthorized access to copyrighted computer software); *Sony Computer Entm't Am., Inc. v. Gamemasters*, 87 F. Supp. 2d 976, 981 (N.D. Cal. 1999) (game console prevented unauthorized operation of video games); *RealNetworks*, Civ. No. 2:99CV02070, 2000 WL 127311, at *3 (authentication sequence prevented unauthorized access to streaming "copyrighted digital works" online).

On the other hand, Congress did not intend the DMCA to apply (and courts are less likely to apply it) where executing a copyrighted computer program creates no protectable expression (as it would for a work in digital form), but instead results in an output that is purely functional. *See*, *e.g.*, *Lexmark*, 387 F.3d at 548 (holding that a computer chip on a replacement printer cartridge that emulates an authentication sequence executing a copyrighted code on a manufacturer's printer cartridge did not violate § 1201(a) because executing the code merely controls printer functions such as "paper feeding," "paper movement," and "motor control" and therefore "is not a conduit to protectable expression"); *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178, 1204 (Fed. Cir. 2004) (holding that use of a transmitter to emulate a copyrighted computer code in a garage door opener did not violate § 1201(a) because executing the code merely performed the function of opening the garage door).

Accordingly, prosecutors should bear in mind that courts are more inclined to rule that a defendant violated § 1201(a) if his conduct occurred in a context to which Congress intended the statute to apply—i.e., when it involves an access control that protects access to copyrighted expression stored in digital form. For questions on this often technical point, prosecutors may wish to consult CCIPS at (202) 514-1026.

V.B.1.e. Regulatory Exemptions to Liability Under § 1201(a)(1)

Before prosecuting a charge of unlawful access control circumvention, § 1201(a)(1)(A), prosecutors should confirm whether the defendant's actions fall within the Librarian of Congress's latest regulatory exemptions.

Because Congress was concerned that the DMCA's prohibitions against circumventing access controls might affect citizens' noninfringing uses of works in unforeseeable and adverse ways, Congress created a recurring rulemaking proceeding to begin two years after the DMCA's enactment and every three years thereafter. 17 U.S.C. § 1201(a)(1)(C), (D). Specifically, the DMCA provides that its prohibition on access circumvention itself, 17 U.S.C. § 1201(a)(1)(A), will not apply to users control of certain types of works if, upon the recommendation of the Register of Copyrights, the Librarian of Congress concludes that the ability of those users "to make noninfringing uses of [a] particular class of work[]" is "likely to be ... adversely affected" by the prohibition. 17 U.S.C. § 1201(a)(1)(B). The statute makes clear, however, that any exceptions to § 1201(a)(1)(A) adopted by the Librarian of Congress are not defenses to violations of the anti-trafficking provisions contained in §§ 1201(a)(2) and 1201(b). *See* 17 U.S.C. § 1201(a)(1)(E).

The current exemptions, effective from October 28, 2003, until October 27, 2006, are

- compilations containing lists of blocked Web sites intended to prevent access to domains, Web sites, or portions of Web sites (but not lists of Internet locations blocked by software designed to protect against damage to computers, such as firewalls and antivirus software, or software designed to prevent receipt of unwanted e-mail, such as anti-spam software).

- computer programs protected by dongles—security or copy protection devices for commercial microcomputer programs—that prevent access due to malfunction or damage and which are obsolete.

- "computer programs and video games distributed in formats that have become obsolete and th[at] require[] original media or hardware as a condition of access."

- "literary works distributed in e-book format when all existing e-book editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling of the e-book's read-aloud function and that prevent the enabling of screen readers to render the text into a 'specialized format.'"

See 37 C.F.R. § 201.40 (2003). The next rulemaking will occur in 2006.

V.B.2. Trafficking in Access Control Circumvention Tools and Services—17 U.S.C. §§ 1201(a)(2) and 1204

In addition to prohibiting the circumvention of access controls, the DMCA also prohibits the manufacture of, or trafficking in, any technology that circumvents access controls without the copyright owner's permission. 17 U.S.C. § 1201(a)(2). To prove a violation of 17 U.S.C. §§ 1201(a)(2) and 1204, the government must establish that the defendant

1. willfully
2. manufactured or trafficked in
3. a technology, product, service, or part thereof
4. that either:
    a. is primarily designed or produced for the purpose of
    b. "has only limited commercially significant purpose or use other than" or
    c. "is marketed by that person or another acting in concert with that person with that person's knowledge for use in"
5. circumventing an access control without authorization from the copyright owner
6. for commercial advantage or private financial gain.

For purposes of the DMCA, prosecutors may look to the law of copyright infringement for guidance regarding the "willfully" element and the "commercial advantage" element, discussed in Chapter II of this Manual. For a complete discussion of establishing the element regarding circumventing an access control, see Sections V.B.1.a.-e. of this Chapter. The Federal Circuit's additional element for establishing a violation of § 1201(a)(2)—that the unauthorized access must also infringe or facilitate infringing a right protected by the Copyright Act—is discussed in Section V.B.1.

V.B.2.a. Trafficking

Section 1201(a)(2) states that "[n]o person shall manufacture, import, offer to the public, provide, or otherwise traffic in" a technology or service that unlawfully circumvents an access control. To "traffic" in such technology means to engage either in dealings in that technology or service or in conduct that necessarily involves awareness of the nature of the subject of the trafficking. *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 325 (S.D.N.Y. 2000). To "provide" technology means to make it available or to furnish it. *Id.* The phrase "or otherwise traffic in" modifies and gives meaning to the words "offer" and "provide." *Id.* Thus, "the anti-trafficking provision of the DMCA is implicated where one presents, holds out or makes a circumvention technology or device available, knowing its nature, for the purpose of allowing others to acquire it." *Id.* This standard for "trafficking," therefore, hinges on evaluating the trafficker's purpose for making the circumvention technology available. *See id.* at 341 n.257 ("In evaluating purpose, courts will look at all relevant circumstances."). Significantly, however, the government need not prove "an intent to cause harm" to establish the trafficking element. *Cf. Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 457 (2d Cir. 2001).

This standard is particularly helpful for determining whether a defendant has trafficked online in unlawful circumvention technology. For example, courts may view a defendant's trafficking to include offering circumvention technology for download over the Internet, or posting links to Web sites that automatically download such technology when a user is transferred by hyperlink, where the purpose of such linking is to allow others to acquire the circumvention technology. *See, e.g., Reimerdes*, 111 F. Supp. 2d at 325, 341 n.257 (holding that offering and providing for download a computer program to circumvent DVD access controls for the purpose of disseminating the program satisfies trafficking element of § 1201(a)(2)). In addition, at least one court has found that posting a hyperlink to web pages "that display nothing more than the [circumventing] code or present the user only with the choice of commencing a download of [the code] and no other content" also constitutes "trafficking" under the DMCA because the defendant's express purpose in linking to these web pages was to disseminate the circumventing technology. *Id.* at 325.

In contrast, posting a link to a web page that happens to include, among other content, a hyperlink for downloading (or transferring to a page for downloading) a circumvention program would not, alone, constitute "trafficking" in the program "regardless of purpose or the manner in which the link was described." *Id.*; *see also id.* at 341 n.257 ("A site that deep links to a page containing only [the circumventing program] located on a site that contains a broad range of other content, all other things being equal, would more likely be found to have linked for the purpose of disseminating [the program] than if it merely links to the home page of the linked-to site."). This result is consistent with the general principle that a website owner cannot be held responsible for all the content of the sites to which it provides links. *Id.* at 325 n.180 (quotation omitted). Thus, posting a link (or "linking") to a circumvention program could constitute "trafficking" if the person linking to the program 1) knew that the program is on the linked-to site; 2) knew that the program constituted unlawful circumvention technology; and 3) posted the link for the purpose of disseminating that technology. *See id.* at 325, 341.

V.B.2.b. In a Technology, Product, Service, or Part Thereof

Section 1201(a)(2) prohibits trafficking "in any technology, product, service, device, component, or part thereof" that unlawfully circumvents access controls. This language is "all-encompassing: it includes any tool, no matter its form, that is primarily designed or produced to circumvent technological protection." *United States v. Elcom*, 203 F. Supp. 2d 1111, 1123 (N.D. Cal. 2002). This element is not limited to conventional devices but instead includes "any technology," including computer code and other software, capable of unlawful circumvention. *Reimerdes*, 111 F. Supp. 2d at 317 & n.135. In addition, the government satisfies this element even if only one "part" or feature of the defendant's technology unlawfully circumvents access controls. *See 321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1098 (N.D. Cal. 2004).

V.B.2.c. Purpose or Marketing of Circumvention Technology

Section 1201(a)(2) prohibits trafficking in technology that unlawfully circumvents access controls and either "is primarily designed or produced for th[at] purpose," "has only limited commercially significant purpose or use other than" such purpose; or is knowingly marketed for such purpose. 17 U.S.C. § 1201(a)(2)(A)-(C). Thus, "only one of the[se] three enumerated conditions must be met" to satisfy this element. *See 321 Studios*, 307 F. Supp. 2d at 1094. And, as noted elsewhere, the fact that a particular circumvention technology is capable of substantial noninfringing uses is not a defense to trafficking in technology that circumvents access controls and violates one of the three conditions enumerated in § 1201(a)(2)(A)-(C). *See RealNetworks, Inc. v. Streambox, Inc.*, No. 2:99CV02070, 2000 WL 127311, at *8 (W.D. Wash. Jan. 18, 2000).

V.B.2.c.1. Primarily Designed or Produced

Trafficking in circumvention technology violates § 1201(a)(2)(A) where its "primary purpose" is to circumvent technological measures controlling access to, for example, copyrighted video games (*Davidson & Assocs. v. Jung*, 422 F.3d 630, 641 (8th Cir. 2005); *Sony Computer Entm't Am., Inc. v. Gamemasters*, 87 F. Supp. 2d 976, 987 (N.D. Cal. 1999)), copyrighted streaming video or music content (*Streambox*, No. 2:99CV02070, 2000 WL 127311, at *7-*8), and copyrighted movies encrypted onto DVDs (*Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 318-19 (S.D.N.Y. 2000); *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1098 (N.D. Cal. 2004)).

Whether a technology's "primary purpose" is to circumvent an access control is determined by the circumvention technology's primary function, not the trafficker's subjective purpose. The defendant's subjective motive may, however, affect whether his conduct falls within one of the DMCA's statutory exceptions. See Section V.C. of this Chapter.

In *Reimerdes*, which concerned the CSS DVD-encryption scheme, the court found that "(1) CSS is a technological means that effectively controls access to plaintiffs' copyrighted works, (2) the one and only function of [the defendant's program] is to circumvent CSS, and (3) defendants offered and provided [the program] by posting it on their web site." *Reimerdes*, 111 F. Supp. 2d at 319. The court held that it was "perfectly obvious" that the program "was designed primarily to circumvent CSS." *Id.* at 318. Defendants argued that their program was not created for the "purpose" of pirating copyrighted movies, but rather to allow purchasers of DVDs to play them on unlicensed DVD players running the Linux operating system. *Id.* at 319. As the court held, however, "whether the development of a Linux DVD player motivated those who wrote [the program] is immaterial to the question" of whether the defendants "violated the anti-trafficking provision[s] of the DMCA." *Id.* The trafficking "of the program is the prohibited conduct—and it is prohibited irrespective of why the program was written." *Id.*

V.B.2.c.2. Limited Commercially Significant Purpose Other Than Circumvention

___Whether a technology has only limited commercially significant purpose other than circumvention is a separate inquiry from whether its primary purpose was to circumvent, and it requires a fact-specific inquiry that often hinges on whether the circumvention technology is "free and available." Some courts, however, have ruled that a particular technology "is primarily designed or produced for the purpose of circumventing" access controls (§ 1201(a)(2)(A)) and also "has only limited commercially significant purpose" other than such circumvention (§ 1201(a)(2)(B)). *See*, *e.g.*, *Davidson*, 422 F. 3d at 641 (holding that defendant's circumvention technology "had limited commercial purpose because its sole purpose was ... circumventing [the] technological measures controlling access to Battle.net and the [computer] games"); *Streambox*, No. 2:99CV02070, 2000 WL 127311, at *8 (holding that defendant violated §§ 1201(a)(2)(A) and (a)(2)(B) by trafficking in circumvention technology that had "no significant commercial purpose other than to enable users to access and record protected content"). However, at least one court suggested that whether a defendant violates § 1201(a)(2)(B) "is a question of fact for a jury to decide," even where the court otherwise finds that the defendant has violated § 1201(a)(2)(A). *321 Studios*, 307 F. Supp. 2d at 1098.

V.B.2.c.3. Knowingly Marketed for Circumvention

When accused of having marketed technology for use in circumventing access controls in violation of § 1201(a)(2)(C), defendants have raised First Amendment defenses—particularly where only a part of a product circumvents access controls—contending that marketing the product may include dissemination of information about the product's other, legal attributes. Although a more complete discussion analyzing the DMCA's validity under the First Amendment is discussed in Section V.C.10.b. of this Chapter, it is worth noting here that "the First Amendment does not protect commercial speech that involves illegal activity," even if that commercial speech is merely instructions for violating the law. *321 Studios*, 307 F. Supp. 2d at 1098-99 (citing *Florida Bar v. Went For It, Inc.*, 515 U.S. 618, 623-24 (1995)); *see also Corley*, 273 F.3d at 447 (citing *United States v. Raymond*, 228 F.3d 804, 815 (7th Cir. 2000) (holding that "First Amendment does not protect instructions for violating the tax laws")). Thus, knowingly marketing technology for use in circumventing access controls in violation of § 1201(a)(2)(C) constitutes illegal activity, and hence, unprotected speech. *321 Studios*, 307 F. Supp. 2d at 1099 ("[A]s 321 markets its software for use in circumventing CSS, this Court finds that 321's DVD copying software is in violation of the marketing provisions of §§ 1201(a)(2) and (b)(1).").

V.B.3. Trafficking in Tools, Devices, and Services to Circumvent Copy Controls—17 U.S.C. §§ 1201(b)(1) and 1204

As noted above, the DMCA prohibits the manufacture or trafficking in any technology that circumvents copy controls without the copyright owner's permission. 17 U.S.C. § 1201(b)(1). To prove a violation of 17 U.S.C. §§ 1201(b)(1) and 1204, the government must establish that the defendant

1. willfully
2. manufactured or trafficked in
3. a technology, product, service, or part thereof
4. that either:
   a. "is primarily designed or produced for the purpose of"
   b. "has only limited commercially significant purpose or use other than" or
   c. "is marketed by that person or another acting in concert with that person with that person's knowledge for use in"
5. "circumventing"
6. "protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof"
7. "for commercial advantage or private financial gain."

See 17 U.S.C. §§ 1201(a)(2)(A)-(C), 1204. For purposes of the DMCA, prosecutors may look to the law of copyright infringement for guidance regarding the "willfully" element and the "commercial advantage" element. See Chapter II of this Manual. In addition, because the second, third, and fourth elements of a § 1201(b) violation operate in the same way as do the comparable elements of a § 1201(a) violation, a complete discussion of those elements may be found in Sections V.B.1. and V.B.2. of this Chapter.

V.B.3.a. Circumventing

To "circumvent protection afforded by a technological measure," as set forth in 17 U.S.C. § 1201(b), "means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure." 17 U.S.C. § 1201(b)(2)(A). To establish this element, the government must show that the defendant trafficked in technology allowing the end user to bypass a copy or use control that "effectively protects the right of a copyright owner." 17 U.S.C. § 1201(b)(1), (b)(2)(B). Courts have found that the following technologies circumvent copy controls: (1) a computer program that removes user restrictions from an "ebook" to make such files "readily copyable" and "easily distributed electronically," *United States v. Elcom*, 203 F. Supp. 2d 1111, 1118-19 (N.D. Cal. 2002); (2) technology that bypasses copy controls intended to prevent the copying of streaming copyrighted content, *RealNetworks, Inc. v. Streambox, Inc.*, No. 2:99CV02070, 2000 WL 127311, at *6-*8 (W.D. Wash. Jan. 18, 2000); and (3) technology that bypasses a scheme intended to "control copying of [encrypted] DVDs," *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1097 (N.D. Cal. 2004). Further, at least one court has held that an unlicensed DVD player that can bypass a DVD's access and copy controls unlawfully "avoids and bypasses" (i.e., circumvents) the DVD's copy control pursuant to § 1201(b)(2)(A). *Id.* at 1098.

V.B.3.b. Technological Measure That Effectively Protects a Right of a Copyright Owner Under This Title ("Copy Control")

"[A] technological measure 'effectively protects a right of a copyright owner under this title' if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title." 17 U.S.C. § 1201(b)(2)(B). The "rights of a copyright owner" include all the exclusive rights set forth in 17 U.S.C. § 106: the rights to reproduce the copyrighted work, to prepare derivative works based upon the copyrighted work, to distribute copies by sale or otherwise, to perform the copyrighted work publicly, and to display the copyrighted work publicly. *Elcom*, 203 F. Supp. 2d at 1124. Thus, a technological measure "effectively protects the right of a copyright owner if, in the ordinary course of its operation, it prevents, limits or otherwise restricts the exercise of any of the rights set forth in [§] 106." *See id.* at 1124; *Agfa Monotype Corp. v. Adobe Sys., Inc.*, 404 F. Supp. 2d 1030, 1039 (N.D. Ill. 2005) (holding that computer font embedding bits do not protect the rights of a copyright owner where "[s]uch embedding bits do not prevent copying, and a computer program can simply proceed to copy the ... [f]ont data regardless of the setting of the bit").

Notably, the government has successfully taken the position that although fair use normally limits a copyright owner's right to claim infringement, § 1201(b)(1) nonetheless prohibits trafficking in *all* tools that circumvent copy controls, even if such tools circumvent copy protections for the purpose of facilitating fair uses of a copyrighted work. *See*, *e.g.*, *Elcom*, 203 F. Supp. 2d at 1124 ("Nothing within the express language would permit trafficking in devices designed to bypass use restrictions in order to enable a fair use, as opposed to an infringing use."). Hence, § 1201(b)(1) bans trafficking in all tools that are primarily designed or produced for the purpose of circumventing copy controls, regardless of whether the downstream use of such tools is infringing or not. *See id.* "It is the technology itself at issue, not the uses to which the copyrighted material may be put." *321 Studios*, 307 F. Supp. 2d at 1097. This is consistent with Congress's intent in enacting the DMCA: "Congress did not ban the act of circumventing the use restrictions. Instead, Congress banned only the trafficking in and marketing of devices primarily designed to circumvent the use restriction protective technologies. Congress did not prohibit the act of circumvention because it sought to preserve the fair use rights of persons who had lawfully acquired a work." *Elcom*, 203 F. Supp. 2d at 1120 (emphasis omitted); *see also Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 443 (2d Cir. 2001) ("[T]he DMCA targets the circumvention of digital walls guarding copyrighted material (and trafficking in circumvention tools), but does not concern itself with the use of those materials after circumvention has occurred.") (emphasis and citations omitted).

Accordingly, while it is not unlawful to *circumvent* a copy or usage control for the purpose of engaging in fair use, it is unlawful under § 1201(b)(1) to *traffic* in tools that allow fair use circumvention. *Elcom*, 203 F. Supp. 2d at 1125. Further, "legal downstream use of the copyrighted material by customers is not a defense to the software manufacturer's violation of the provisions of § 1201(b)(1)." *321 Studios*, 307 F. Supp. 2d at 1097-98.

V.B.4. Alternate § 1201(b) Action—Trafficking in Certain Analog Videocassette Recorders and Camcorders

Congress's decision to include a prohibition regarding analog technology may be a *non sequitur* in an act entitled the "Digital Millennium Copyright Act." Nonetheless, § 1201(k)(5) of the DMCA prescribes that any violation of 17 U.S.C. § 1201(k)(1) regarding copy controls on certain analog recording devices "shall be treated as a violation of" § 1201(b)(1). Section 1201(k)(1)(A) proscribes trafficking in any VHS, Beta, or 8mm format analog video cassette recorder or 8mm analog video cassette camcorder unless such recorder or camcorder "conforms to the automatic gain control copy control technology." 17 U.S.C. § 1201(k)(1)(A)(i)-(iv). The same prohibition applies to any "analog video cassette recorder that records using an NTSC format video input." 17 U.S.C. § 1201(k)(1)(A)(v). Section 1201(k)(1)(B) also prohibits trafficking in any VHS or 8mm format analog video cassette recorder if the recorder's design (previously conforming with § 1201(k)(1)(A)) was modified to no longer conform with automatic gain control copy technology. 17 U.S.C. § 1201(k)(1)(B)(i). Similarly, the DMCA prohibits trafficking in such an analog video cassette recorder if it "previously conformed to the four-line colorstripe copy control technology" but was later modified so that it "no longer conforms to such technology." 17 U.S.C. § 1201(k)(1)(B)(ii). In addition, the DMCA requires "manufacturers that have not previously manufactured or sold VHS [or 8mm] format analog video cassette recorder[s] to conform to the four-line colorstripe copy control technology." *Id.*

Notably, § 1201(k) does not (1) require analog camcorders to conform to the automatic gain control copy control technology for video signals received through a camera lens; (2) apply to the manufacture or trafficking in any "professional analog video cassette recorder;" or (3) apply to transactions involving "any previously owned analog video cassette recorder" that had been both legally manufactured and sold when new and also not later modified to violate § 1201(k). 17 U.S.C. § 1201(k)(3)(A)-(C).

V.B.5. Falsifying, Altering, or Removing Copyright Management Information—17 U.S.C. § 1202

Section 1202 prohibits anyone from knowingly falsifying, removing, or altering "copyright management information"—such as a copyrighted work's title, copyright notice, or author—with the intent to induce, enable, facilitate, or conceal infringement. 17 U.S.C. § 1202(a)(1), (b)(1), (c) (defining "copyright management information"). Section 1202 further prohibits intentionally facilitating infringement by knowingly distributing or importing for distribution (1) false copyright management information or (2) copyright management information knowing that such information has been removed or altered without authority. 17 U.S.C. § 1202(a)(2), (b)(2). Finally, § 1202 prohibits anyone from intentionally facilitating infringement by distributing, importing for distribution, or publicly performing copyrighted works, copies of works, or phonorecords knowing that their copyright management information has been removed or altered without authority. 17 U.S.C. § 1202(b)(3).

Thus, while § 1201 primarily targets circumvention devices and technology, "Section 1202 imposes liability for specified acts. It does not address the question of liability for persons who manufacture devices or provide services." H.R. Rep. No. 105-551 (I), at 22 (1998). Like § 1201, however, to establish a criminal violation of § 1202, the government must prove two elements in addition to those in the statute itself—that the defendant violated § 1202 both (1) willfully and (2) for purposes of commercial advantage or private gain. 17 U.S.C. § 1204(a).

Criminal enforcement of § 1202 of the DMCA is rare, and prosecutors are encouraged to contact CCIPS at (202) 514-1026 for guidance when considering a charge under this provision.

V.C. Defenses

The DMCA provides for several statutory defenses, exceptions, and even "exemptions" to the anti-circumventing and anti-trafficking prohibitions set forth in 17 U.S.C. § 1201. As the following discussion demonstrates, these defenses do not apply uniformly to the anti-circumvention (§ 1201(a)(1)(A)) and anti-trafficking provisions (§ 1201(a)(2), (b)).

V.C.1. Statute of Limitations

Section 1204(c) of the DMCA states that "[n]o criminal proceeding shall be brought under this section unless such proceeding is commenced within 5 years after the cause of action arose." 17 U.S.C. § 1204(c).

V.C.2. Librarian of Congress Regulations

The Librarian of Congress promulgates regulatory exemptions every three years that apply only to § 1201(a)(1)(A)'s prohibitions against circumventing access controls. See Section V.B.1.e. of this Chapter.

V.C.3. Certain Nonprofit Entities

Section 1204(b) exempts from criminal prosecution all nonprofit libraries, archives, educational institutions, or public broadcasting entities as defined by 17 U.S.C. § 118(f). *See also* 17 U.S.C. § 1201(d) (listing other entities). The exception set forth in § 1201(d) for nonprofit libraries, archives, and educational institutions is not as broad as the exemption from criminal prosecution for the same group of entities set forth in § 1204(b), because the latter (1) also includes "public broadcasting entities" and (2) precludes prosecution for the anti-circumvention and the anti-trafficking violations of § 1201.

V.C.4. Information Security Exemption

"[A]ny lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee" or contractor of the federal government or a state government is exempt from all three of § 1201's prohibitions for information security work on "a government computer, computer system, or computer network." 17 U.S.C. § 1201(e). Congress intended that the term "computer system" would have the same meaning in § 1201(e) as it does in the Computer Security Act. H.R. Conf. Rep. No. 105-796, at 66 (1998), *reprinted in* 1998 U.S.C.C.A.N. 639, 643.

This exemption is narrower than it might first appear. Congress intended this exemption to permit law enforcement to lawfully disable technological protection measures protecting copyrighted works (e.g., measures protecting access to copyrighted computer software) to probe internal government computer systems to ensure that they are not vulnerable to hacking. *Id.* at 65. Thus, "information security" consists of "activities carried out in order to identify and address the vulnerabilities of a *government* computer, computer system, or computer network." 17 U.S.C. § 1201(e) (emphasis added); *see also id.* at 66.

V.C.5. Reverse Engineering and Interoperability of Computer Programs

Section 1201(f) contains three reverse engineering or "interoperability" defenses for individuals using circumvention technology "for the sole purpose of trying to achieve 'interoperability'" of computer programs through reverse engineering. *Davidson & Assocs. v. Jung*, 422 F.3d 630, 641-42 (8th Cir. 2005). Note that at least one court has held that reverse engineering can satisfy the statutory fair use exception. *Bowers v. Baystate Techs., Inc.*, 320 F.3d 1317, 1325 (Fed. Cir. 2003).

The key term for these defenses, "interoperability," "means the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged." 17 U.S.C. § 1201(f)(4). The scope of these exemptions is expressly limited to "computer programs" and does not authorize circumvention of access controls that protect other classes of copyrighted works, such as movies. *Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 2d 211, 218 (S.D.N.Y. 2000).

The first interoperability defense allows a person "who has lawfully obtained the right to use a copy of a computer program ... for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to th[at] person" to circumvent an access control without violating the DMCA's anti-circumvention prohibition set forth in § 1201(a)(1)(A). 17 U.S.C. § 1201(f)(1). By definition, this exemption does not apply to one who obtains a copy of the computer program illegally.

Second, § 1201(f)(2) exempts violations of the DMCA's anti-trafficking provisions (§ 1201(a)(2), (b)) for those who "develop and employ technological means" that are "necessary" to enable interoperability. Despite the statute's express requirement that this defense only applies "if such means are necessary to achieve such interoperability," 17 U.S.C. § 1201(f)(2), at least one court has held that "the statute is silent about the degree to which the 'technological means' must be necessary, if indeed they must be necessary at all, for interoperability." *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 551 (6th Cir. 2004).

Third, § 1201(f)(3) authorizes one who acquires information through § 1201(f)(1) to make this information and the technical means permitted under § 1201(f)(2) available to others "solely for the purpose of enabling interoperability of an independently created computer program with other programs." 17 U.S.C. § 1201(f)(3). Significantly, § 1201(f)(3) "permits information acquired through reverse engineering to be made available to others *only by the person who acquired the information*." *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 320 (S.D.N.Y. 2000) (emphasis added). Consequently, one court disallowed this defense because, *inter alia*, the defendants "did not do any reverse engineering [themselves]. They simply took [the program] off someone else's web site and posted it on their own." *Id.*

None of these defenses apply if the defendant's conduct also constituted copyright infringement or, in the case of the third defense, otherwise "violate[d] applicable law." *See* 17 U.S.C. § 1201(f)(1)-(3); *see also Lexmark*, 387 F.3d at 551 (holding that defendant, which produced a computer chip that allowed a remanufactured printer cartridge to interoperate with another's originally manufactured printer, did not commit infringement because the computer program that defendant had copied from plaintiff was not copyrighted).

To establish a violation of the anti-trafficking provisions, prosecutors need not establish that the defendant's motive for manufacturing or trafficking in a circumvention tool was to infringe or to permit or encourage others to infringe. *See Reimerdes*, 111 F. Supp. 2d at 319. In contrast, to determine whether defendants meet the interoperability exemption, prosecutors must determine whether the defendant's motive for developing or trafficking the technological means for circumventing an access or copy control was "solely for the purpose" of achieving or enabling interoperability. *Id.* at 320.

Courts strictly apply the requirement that circumvention and dissemination occur "solely for the purpose" of achieving interoperability and not to facilitate copyright infringement. For example, one court has held that circumventing a copyrighted computer game's access controls for the purpose of developing and disseminating a copy or "emulator" that was essentially identical to the original but lacked the original's access control, "constituted more than enabling interoperability" under § 1201(f)(1) and "extended into the realm of copyright infringement." *Davidson & Assoc. Inc. v. Internet Gateway, Inc.*, 334 F. Supp. 2d 1164, 1185-86 (E.D. Mo. 2004) ("The defendants' purpose in developing the bnetd server was to avoid the anti-circumvention restrictions of the game and to avoid the restricted access to Battle.net. Thus, the sole purpose of the [] emulator was not to enable interoperability."), *aff'd*, 422 F.3d at 642 ("Appellant's circumvention in this case constitutes infringement."); *cf. Reimerdes*, 111 F. Supp. 2d at 320 (holding that the purpose of [the defendant's program] was simply to decrypt DVD access controls and not, as defendants claimed, to achieve interoperability between computers running Linux operating system because [the program] also could be used to decrypt and play DVDs on unlicensed players running the Windows operating system). In addition, where the development (or distribution to the public) of circumvention technology itself constitutes copyright infringement, the DMCA expressly precludes reliance on § 1201(f)(2) and (3). *See id.* (holding that "[t]he right to make the information available extends only to dissemination 'solely for the purpose' of achieving interoperability as defined by the statute. It does not apply to public dissemination of means of circumvention") (footnote omitted).

Moreover, legislative history suggests that the "independently created [computer] program" referenced in this exemption must not infringe the original computer program and instead must be "a new and original work."

H.R. Rep. No. 105-551 (II), at 42 (1998). Thus, if the defendant's functionally equivalent computer program is "new and original" only insofar as it lacks the original's access controls, then the defendant has not created an "independently created computer program." *Davidson*, 334 F. Supp. 2d at 1185, *aff'd*, 422 F.3d at 642. If, on the other hand, the defendant's program actually performs functions that the original program did not, courts are more inclined to find that defendants have satisfied the "independently created computer program" requirement. *Lexmark*, 387 F.3d at 550 (holding that even though remanufacturer's toner cartridge chip contained "exact copies" of original manufacturer's computer program, it was nonetheless an "independently created computer program" because it "contain[s] other functional computer programs beyond the copied" original program). The independent program need not have already existed before the defendant reverse-engineered the original program. *Id.* at 550-51 (holding that "nothing in the statute precludes simultaneous creation of an interoperability device and another computer program" so long as it is "'independently' created").

V.C.6. Encryption Research

Certain encryption research is exempted from liability under § 1201(a) (but *not* from § 1201(b)). *Reimerdes*, 111 F. Supp. 2d at 321 n.154. For purposes of this exemption, "encryption research" consists of "activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products." 17 U.S.C. § 1201(g)(1)(A). The phrase, "encryption technologies," "means the scrambling and descrambling of information using mathematical formulas or algorithms." 17 U.S.C. § 1201(g)(1)(B).

The first encryption research exemption is that it is not a violation of the anti-circumvention provision (§ 1201(a)(1)(A)) where a defendant "circumvent[s] a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if" four conditions are satisfied: (1) he "lawfully obtained" the applicable encrypted published work; (2) the circumvention "is necessary to conduct such encryption research;" (3) he "made a good faith effort to obtain authorization before the circumvention;" and (4) the circumvention does not constitute copyright infringement "or a violation of applicable law," including the Computer Fraud Abuse Act of 1986, 18 U.S.C. § 1030. 17 U.S.C. § 1201(g)(2).

To determine whether a defendant qualifies for this exemption, courts consider the following non-exclusive factors: (1) whether the results of the putative encryption research are disseminated in a manner designed to advance the state of knowledge of encryption technology versus facilitation of copyright infringement; (2) whether the person in question is engaged in legitimate study of or work in encryption; and (3) whether the results of the research are communicated in a timely fashion to the copyright owner. 17 U.S.C. § 1201(g)(3).

The second encryption research exemption is that a defendant does not violate the access control anti-trafficking provision (§ 1201(a)(2)) for developing and distributing tools, such as software, that are needed to conduct permissible encryption research as described in the first encryption research exemption in § 1201(g)(2). 17 U.S.C. § 1201(g)(4); H.R. Rep. No. 105-551 (II), at 44 (1998). This exemption essentially frees an encryption researcher to cooperate with other researchers, and it also allows one researcher to provide the technological means for such research to another to verify the research results. *Id.*

It is not a violation of § 1201(a)(2) for a person to (1) "develop and employ technological means to circumvent a technological measure for the sole purpose of that person performing the acts of good faith encryption research described in" § 1201(g)(2) and (2) "provide the technological means to another person with whom he is or she is working collaboratively" for the purpose of either conducting good faith encryption research or having another person verify such research as described in § 1201(g)(2). 17 U.S.C. § 1201(g)(4).

This exemption is quite complex and has been relied upon infrequently in reported decisions. For a report on the early effects of this exemption (or lack thereof) on encryption research and on protection of content owners against unauthorized access of their encrypted copyrighted works, see the "*Report to Congress: Joint Study of Section 1201(g) of The Digital Millennium Copyright Act*" prepared by the U.S. Copyright Office and the National Telecommunications and Information Administration of the Department of Commerce pursuant to § 1201(g)(5), *available at* http://www.copyright.gov/reports/studies/ dmca_report.html.

V.C.7. Restricting Minors' Access to the Internet

Section 1201(h) creates a discretionary exception, giving the court discretion to waive violations of §§ 1201(a)(1)(A) and 1201(a)(2) so that those prohibitions are not applied in a way that "inadvertently make[s] it unlawful for parents to protect their children from pornography and other inappropriate material available on the Internet, or have unintended legal consequences for manufacturers of products designed solely to enable parents to protect their children." H.R. Rep. No. 105-551 (II), at 45 (1998). Specifically, § 1201(h) authorizes the court to "consider the necessity for its intended and actual incorporation in a technology, product, service, or device, which (1) does not itself violate the provisions of this title; and (2) has the sole purpose to prevent the access of minors to material on the Internet." 17 U.S.C. § 1201(h). Congress was concerned that if Internet filtering tools are developed in the future that incorporate a part or component that circumvent access controls to a copyrighted work "solely in order to provide a parent with the information necessary to ascertain whether that material is appropriate for his or her child, this provision authorizes a court to take into consideration the necessity for incorporating such part or component in a suit alleging a violation of section 1201(a)." S. Rep. No. 105-190, at 14 (1998).

To date, no reported case has applied this discretionary exception.

V.C.8. Protection of Personally Identifying Information

Section 1201(i)(1) states that it is not a violation of § 1201(a)(1)(A) to circumvent an access control for the purpose of disabling files that collect personally identifiable information like "'cookie files'—which are automatically deposited on hard drives of computers of users who visit World Wide Web sites." *Id.* at 18. However, if a copyright owner conspicuously discloses that its access control also contains personal data gathering capability, and if the consumer is given the ability to effectively prohibit that gathering or dissemination of personal information, then this exception does not apply and no circumvention is permitted. H.R. Rep. No. 105-551 (II), at 45 (1998). Further, if the copyright owner conspicuously discloses that neither the access control nor the work it protects collect personally identifying information, then no circumvention is permitted. 17 U.S.C. § 1201(i)(2). Note that this exception does not apply to the anti-trafficking prohibitions.

V.C.9. Security Testing

A person who engages in good faith "security testing" does not violate § 1201(a). 17 U.S.C. § 1201(j). "Security testing" consists of "accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network." 17 U.S.C. § 1201(j)(1).

Without such authorization, a defendant cannot qualify for this exemption. *Reimerdes*, 111 F. Supp. 2d at 321. A defendant engaging in security testing does not violate § 1201(a)(1)(A) so long as such testing does not constitute copyright infringement nor a violation of other applicable law such as the Computer Fraud and Abuse Act of 1986. 17 U.S.C. § 1201(j)(2). In evaluating this exemption, the DMCA requires a court to consider whether the information derived from the security testing (1) "was used solely to promote the security of the owner or operator of [or shared directly with the developer of] such computer, computer system or computer network, or" (2) "was used or maintained in a manner that does not facilitate copyright infringement" or a violation of other applicable law. 17 U.S.C. § 1201(j)(3).

Likewise, a defendant does not violate § 1201(a)(2) for trafficking in a "technological means for the sole purpose of performing the acts of security testing" if the testing does not "otherwise violate section (a)(2)." 17 U.S.C. § 1201(j)(4).

V.C.10. Constitutionality of the DMCA

Civil and criminal defendants have repeatedly challenged the constitutionality of Title I of the DMCA, particularly 17 U.S.C. §§ 1201(a)(2) and 1201(b). Defendants have repeatedly challenged Congress's authority, for example, to enact the DMCA pursuant to the Commerce Clause and Intellectual Property Clause. None of these challenges has yet prevailed.

V.C.10.a. Congress's Constitutional Authority to Enact § 1201 of the DMCA

Congress enacted § 1201 pursuant to its authority under the Commerce Clause. See U.S. Const., art. I, § 8, cl. 3; H.R. Rep. No. 105-551 (II), at 22, 35 (1998). Federal courts have uniformly upheld this authority. *See*, *e.g.*, *United States v. Elcom*, 203 F. Supp. 2d 1111, 1138 (N.D. Cal. 2002) ("Congress plainly has the power to enact the DMCA under the Commerce Clause."); *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1103 (N.D. Cal. 2004) (same). Article I, Section 8, Clause 3 of the Constitution delegates to Congress the power "[t]o regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes." Congress does not exceed its Commerce Clause authority where a rational basis exists "for concluding that a regulated activity sufficiently affected interstate commerce." *United States v. Lopez*, 514 U.S. 549, 558 (1995) (citations omitted). The DMCA prohibits circumventing access controls and the trafficking in technology that facilitates circumvention of access or copy controls—the type of conduct that has a substantial effect on commerce between the states and commerce with foreign nations. *See 321 Studios*, 307 F. Supp. 2d at 1103. Congress created the DMCA's anti-trafficking prohibitions to directly regulate specific items moving in commerce (circumvention technology) and to protect channels of interstate commerce, including electronic commerce. H.R. Rep. No. 105-551(II), at 22 (1998). Most significantly, to the extent that circumvention devices enable criminals to engage in piracy by unlawfully copying and distributing copyrighted works, the sale of such devices has a direct effect on suppressing the market for legitimate copies of the works. *See 321 Studios*, 307 F. Supp. 2d at 1103. Accordingly, Congress had a rational basis for concluding that § 1201 regulates activity that substantially affects interstate commerce and therefore acted within its authority under the Commerce Clause. *See Elcom*, 203 F. Supp. 2d at 1138.

Courts have similarly rejected the argument that the DMCA violates the Intellectual Property Clause. The Commerce Clause authorizes Congress to enact legislation that protects intellectual property rights, even where the Intellectual Property Clause alone does not provide sufficient authority for such legislation. Federal courts have long recognized that while each of the powers of Congress is alternative to all of the others, "what cannot be done under one of them may very well be doable under another." *United States v. Moghadam*, 175 F.3d 1269, 1277 (11th Cir. 1999). Congress may thus use the Commerce Clause as a basis for legislating within a context contemplated by another section of the Constitution (like the Intellectual Property Clause) so long as Congress does not override an otherwise existing Constitutional limitation. *Id.* (holding the criminal anti-bootlegging statute, 18 U.S.C. § 2319A, valid under the Commerce Clause even if it is beyond Congress's authority under the Intellectual Property Clause); *compare Heart of Atlanta Motel v. United States*, 379 U.S. 241 (1964) (upholding public accommodation provisions of the Civil Rights Act of 1964 as valid under the Commerce Clause despite the fact that the Act may have reached beyond Congress's authority under the Fourteenth Amendment) *and South Dakota v. Dole*, 483 U.S. 203, 207 (1987) (holding that Congress could rely on the Spending Clause to impose restrictions that would otherwise exceed Congress's power) *with Railway Labor Executives' Ass'n v. Gibbons*, 455 U.S. 457 (1982) (striking down act by Congress under Commerce Clause that violated Bankruptcy Clause's uniformity requirement). Further, the Intellectual Property Clause "itself is stated in positive terms, and does not imply any negative pregnant" that would suggest "a ceiling on Congress's ability to legislate pursuant to other grants." *Moghadam*, 175 F.3d at 1280 (discussing constitutionality of the criminal anti-bootlegging statute, 18 U.S.C. § 2319A). Moreover, "[e]xtending quasi-copyright protection also furthers the purpose of the Copyright Clause to promote the progress of the useful arts." *Id.*

The DMCA's enactment pursuant to the Commerce Clause was valid because it "is not fundamentally inconsistent with" the purpose of the Intellectual Property Clause. *Elcom*, 203 F. Supp. 2d at 1139-41. Indeed, "Congress viewed the DMCA as 'paracopyright' legislation that could be enacted under the Commerce Clause." *Id.* at 1140. Moreover, protecting copyright owners' rights against unlawful piracy by preventing trafficking in tools that would enable widespread piracy and unlawful infringement (i.e., circumvention tools) is consistent with the Intellectual Property Clause's grant to Congress of the power to "'promote the useful arts and sciences' by granting exclusive rights to authors in their writings." *Id.*

Specifically, courts have rejected the common argument that the DMCA's ban on the sale of circumvention tools violates the Intellectual Property Clause's "limited Times" prohibition. That argument is based on the false premise that the DMCA has the effect of allowing publishers to claim copyright-like protection in copyrighted works, even after they pass into the public domain. Prosecutors should vigorously oppose this flawed argument. Nothing in the DMCA permits a copyright owner to prevent his work from entering the public domain, despite the expiration of the copyright. *Id.* at 1141. As discussed in the copyright chapter, the essence of copyright is the legally enforceable exclusive right to reproduce and distribute copies of an original work of authorship, to make derivative works, and to perform the work publicly for a limited time. *See supra* Chapter II; *see also Elcom*, 203 F. Supp. 2d at 1141; 17 U.S.C. §§ 106, 302, 303. When a copyright expires, so does any protectable intellectual property right in a work's expression. *Elcom*, 203 F. Supp. 2d at 1141. Upon expiration, the user may copy, quote, or republish the expression without any legally enforceable restriction on the use of the expression. *Id.* "Nothing within the DMCA grants any rights to anyone in any public domain work. A public domain work remains in the public domain[,] and any person may make use of the public domain work for any purpose." *321 Studios*, 307 F. Supp. 2d at 1104 (internal quotation marks and citation omitted). Accordingly, the DMCA does not extend any copyright protections beyond the statutory copyright term merely by prohibiting the trafficking in or marketing of circumvention technology. *Id.*

V.C.10.b. The First Amendment

Criminal and civil DMCA defendants have raised both facial and "as applied" First Amendment challenges. Although federal courts have uniformly rejected such challenges, defendants continue to raise them in part because the overbreadth and "as applied" First Amendment tests each can include a fact-dependent component.

V.C.10.b.i. Facial Challenges

Facial First Amendment challenges to § 1201—typically alleging that the statute is unconstitutionally overbroad—fail for at least two reasons. First, the DMCA does not expressly proscribe spoken words or patently expressive or communicative conduct. *See Roulette v. City of Seattle*, 97 F.3d 300, 303 (9th Cir. 1996). "[A] facial freedom of speech attack must fail unless, at a minimum, the challenged statute is directed narrowly and specifically at expression or conduct commonly associated with expression." *Id.* at 305 (citations, and internal quotation marks omitted); *see also Virginia v. Hicks*, 539 U.S. 113, 123 (2003).

Section 1201 of the DMCA, "[b]y its terms," is not directed at expression or conduct associated with expression. *Elcom*, 203 F. Supp. 2d at 1133. Instead, § 1201 is a law of general application focused on the circumvention of access controls and the trafficking in circumvention tools; § 1201's prohibitions are not focused on speech. *Id.*; *see also Anderson v. Nidorf*, 26 F.3d 100, 103-04 (9th Cir. 1994) (holding that California's anti-piracy statute is not subject to facial challenge because, *inter alia*, the statute focused upon infringement for commercial advantage or private financial gain). Accordingly, on this basis alone, "an overbreadth facial challenge [to § 1201] is not available." *Elcom*, 203 F. Supp. 2d at 1133.

Second, even were the DMCA directed at spoken words or expressive conduct—which no court has yet held—such a finding would be insufficient to establish overbreadth as a matter of law. The defendant would still have to independently establish that the DMCA is written so broadly that it infringes unacceptably on the First Amendment rights of third parties. *City Council v. Taxpayers for Vincent*, 466 U.S. 789, 798-99 (1984). The overbreadth doctrine "is, manifestly, strong medicine," to be employed "sparingly and only as a last resort." *Broadrick v. Oklahoma*, 413 U.S. 601, 613 (1973). For this reason, a statute will be declared facially unconstitutional for overbreadth only if the court finds a realistic danger that the statute itself will significantly compromise recognized First Amendment protections of parties not before the court. *See New York State Club Ass'n, Inc. v. City of New York*, 487 U.S. 1, 11 (1988).

The DMCA neither compromises a recognized First Amendment protection of third parties, nor is there a realistic danger that such a compromise would occur. Moreover, § 1201's "plainly legitimate sweep" targets circumvention of access controls and the manufacture or trafficking in circumvention technology, not speech. Thus, it is highly unlikely that defendants could establish the facts necessary to claim that § 1201 is overbroad. *See Elcom*, 203 F. Supp. 2d at 1133.

V.C.10.b.ii. "As Applied" Challenges

First Amendment "as applied" challenges to § 1201 necessarily vary according to the technology at issue in each defendant's particular case. DMCA defendants have often alleged that the DMCA violates the First Amendment when applied to circumvention technology in the form of computer code. Although it is arguable whether computer object code constitutes speech, every federal court that has held that computer code is speech has nonetheless ruled that the anti-trafficking provisions do not violate the First Amendment under an intermediate scrutiny standard because the DMCA (1) is content-neutral; (2) furthers important governmental interests in promoting electronic commerce and protecting the rights of copyright owners; and (3) is sufficiently tailored to achieve these objectives without unduly burdening free speech. *See*, *e.g.*, *Elcom*, 203 F. Supp. 2d at 1126-28 (applying *United States v. O'Brien*, 391 U.S. 367, 376 (1968) ("When 'speech' and 'nonspeech' elements are combined in the same course of conduct, a sufficiently important governmental interest in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms.")).

The DMCA's anti-trafficking provisions are content neutral. *See Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 454 (2d Cir. 2001) (§ 1201(a)(2)); *321 Studios*, 307 F. Supp. 2d at 1100 (§§ 1201(a)(2) and 1201(b)); *Elcom*, 203 F. Supp. 2d at 1128-29 (§ 1201(b)). The principal inquiry in determining whether a statute is content neutral is whether the government has adopted a regulation of speech because of agreement or disagreement with the message it conveys. *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 642 (1994). The government's purpose is the controlling measure. *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989).

By this measure, the DMCA's anti-trafficking provisions are clearly content-neutral. Congress intended the DMCA to target the non-speech, functional components of circumvention technology, *Corley*, 273 F.3d at 454, not to "stifle[] speech on account of its message." *Turner*, 512 U.S. at 641. The DMCA is not a content-based statute that would require strict scrutiny under the First Amendment. *See 321 Studios*, 307 F. Supp. 2d at 1100. In fact, "[t]he reason that Congress enacted the anti-trafficking provision of the DMCA had nothing to do with suppressing particular ideas of computer programmers and everything to do with functionality." *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 329 (S.D.N.Y. 2000).

Ultimately, the DMCA is not concerned with whatever capacity circumvention technology might have for conveying information to a person, and that capacity is what arguably creates the speech component of, for example, decrypting computer code. *See Corley*, 273 F.3d at 454. The DMCA would apply to such code solely because of its capacity to decrypt, for instance, an access control. *Id.* "That functional capability is not speech within the meaning of the First Amendment." *Id.*

A statute that is content neutral is subject to intermediate scrutiny and hence satisfies the First Amendment "if it furthers an important or substantial government interest; if the government interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest." *Turner*, 512 U.S. at 662 (quotation and citation omitted). The government's interest in preventing unauthorized copying of copyrighted works and promoting electronic commerce are unquestionably substantial. *See* H.R. Rep. No. 105-551 (II), at 23 (1998); *Elcom*, 203 F. Supp. 2d at 1129-30; *Corley*, 273 F.3d at 454. Congress enacted the DMCA after evaluating a great deal of evidence establishing that copyright and intellectual property piracy are endemic, especially digital piracy. *See* S. Rep. No. 105-190, at 8 (1998). Thus, by prohibiting circumvention of access controls and the trafficking in circumvention technology, "the DMCA does not burden substantially more speech than is necessary to achieve the government's asserted goals of promoting electronic commerce, protecting copyrights, and preventing electronic piracy." *See 321 Studios*, 307 F. Supp. 2d at 1103 (internal quotation marks and citation omitted).

Finally, courts have uniformly found that the DMCA's anti-trafficking provisions meet the Supreme Court's narrow tailoring requirement that a content-neutral regulation of speech promote a substantial government interest that would be achieved less effectively absent the regulation. *See id.* at 1101. The DMCA's numerous exceptions (see Section V.C. of this Chapter) further demonstrate that Congress narrowly tailored the statute to balance, for instance, the needs of law enforcement, computer programmers, encryption researchers, and computer security specialists against the problems created by circumvention technology. *See* 17 U.S.C. §§ 1201(e)-(g), (j); *Elcom*, 203 F. Supp. 2d at 1130-31.

V.C.10.c. Vagueness

Courts have also rejected challenges to the DMCA under the Fifth Amendment on vagueness grounds. Vagueness may invalidate a statute if the statute either (1) fails to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits, or (2) authorizes or encourages arbitrary and discriminatory enforcement. *City of Chicago v. Morales*, 527 U.S. 41, 56 (1999). Defendants typically argue that the DMCA is vague or otherwise infirm because it bans only those circumvention tools that are primarily designed to circumvent access or copy controls to enable copyright infringement, not those enabling fair uses. *See*, *e.g., Elcom*, 203 F. Supp. 2d at 1122. This issue has arisen with respect to § 1201(b), which prohibits trafficking in any copy control circumvention technology. *Id.* at 1124.

Courts have held, however, that the DMCA is not unconstitutionally vague, because it imposes a blanket ban on all circumvention tools regardless of whether the ultimate purpose for their use is fair or infringing. *Id.* "Congress thus recognized that most uses of tools to circumvent copy restrictions would be for unlawful infringement purposes rather than for fair use purposes and sought to ban all circumvention tools that 'can be used' to bypass or avoid copy restrictions." *Id.* at 1125 (quoting S. Rep. No. 105-190, at 29-30). Moreover, Congress's intent to preserve fair use, *see* § 1201(c), is not inconsistent with a ban on trafficking in circumvention technologies, even those that could be used for fair use purposes rather than infringement. *Id.* Although the DMCA may make certain fair uses in digital works more difficult, the DMCA does not eliminate fair use and in fact expressly permits it. *See id.*; 17 U.S.C. § 1201(c)(1). "Thus, while it is not unlawful to circumvent for the purpose of engaging in fair use, it is unlawful to traffic in tools that allow fair use circumvention." *Elcom*, 203 F. Supp. 2d at 1125. Further, because the DMCA prohibits the trafficking of all circumvention tools, Congress need not expressly tie the use of the tool to an unlawful purpose (as may be required, for instance, in a multi-use device context). *Id.* Accordingly, the DMCA, "as written, allows a person to conform his or her conduct to a comprehensible standard and is thus not unconstitutionally vague." *Id.* (citation omitted).

V.C.10.d. Fair Use

For a more detailed explanation of the fair use doctrine, see Section II.C.5. of this Manual.

Defendants typically style their fair use defense to a DMCA violation as an "as applied" First Amendment challenge. For example, traffickers have raised fair use challenges "as applied" to the First Amendment rights of third-party purchasers of the trafficker's circumvention tools. This type of fair use defense fails for at least three reasons. First, the challengers usually lack standing. "[A] person to whom a statute may constitutionally be applied will not be heard to challenge that statute on the ground that it may conceivably be applied unconstitutionally to others, in other situations not before the Court." *Broadrick v. Oklahoma*, 413 U.S. 601, 610 (1973). Those who traffic in circumvention tools that they do not use cannot assert a fair use defense because they are not engaging in any use—fair or infringing—of a copyrighted work. Simply put, traffickers lack standing to challenge the DMCA's constitutionality based on its application to the traffickers' customers.

Second, even a purchaser who could have standing because he did use a copyrighted work cannot rely on the fair use defense, because the DMCA does not present an issue of infringement. Fair use is an affirmative defense to copyright infringement, something that the user can accomplish only *after* he has first circumvented a work's copy controls. *See*, *e.g.*, *Elcom*, 203 F. Supp. 2d at 1121. The DMCA "targets the circumvention of digital walls guarding copyrighted material (and trafficking in *circumvention* tools), [it] does not concern itself with the *use* of those materials after circumvention has occurred." *Corley*, 273 F.3d at 443. Thus, the DMCA's anti-trafficking provisions are not concerned with purchasers' downstream use of circumvention tools. *See Corley*, 273 F.3d at 442; *321 Studios*, 307 F. Supp. 2d at 1097-98.

Third, no court has held that the fair use doctrine is a categorical constitutional requirement. *Corley*, 273 F.3d at 458 ("[T]he Supreme Court has never held that fair use is constitutionally required."). Fair use is a judicially-created doctrine. *Reimerdes*, 111 F. Supp. 2d at 321. Fair use existed only at common law until Congress codified it in the 1976 Copyright Act at 17 U.S.C. § 107, in order to maintain the common-law status quo. *See* H.R. Rep. No. 94-1476, at 66 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5680.

The fact that the fair use doctrine accommodates First Amendment protections—i.e., that certain fair uses may also be protected under the First Amendment, *cf. Eldred v. Ashcroft*, 537 U.S. 186, 218-20 (2003); *Harper*

& Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 560 (1985)—does not make the fair use doctrine and the First Amendment categorically coextensive. *See Elcom*, 203 F. Supp. 2d at 1134 n.4 ("There is no direct authority for the proposition that the doctrine of fair use is coextensive with the First Amendment, such that 'fair use' is a First Amendment right").

Most significantly, courts have rejected "the proposition that fair use, as protected by the Copyright Act, much less the Constitution, guarantees copying by the optimum method or in the identical format of the original." *Corley*, 273 F.3d at 459. Fair use of copyrighted digital works is still possible under the DMCA, even though copying of such works may prove more difficult. *321 Studios*, 307 F. Supp. 2d at 1102.

In addition, the DMCA does not place an impermissible financial burden on fair users' First Amendment rights. Courts have found that this "financial burden" argument "is both an overstatement of the extent of the fair use doctrine and a misstatement of First Amendment law." *Id.* A statute's financial burden on a speaker renders the statute unconstitutional only if such burden was placed on the speaker because of the speech's content, not because of the speaker's desire to make the speech. *Id.* (citations omitted). Section 1201 of the DMCA does not eliminate fair use nor prevent anyone from engaging in traditional methods of fair use such as "quoting from a work or comparing texts for the purpose of study or criticism." *Elcom*, 203 F. Supp. 2d at 1134.

Finally, courts have rejected the argument that the DMCA impairs an alleged First Amendment fair use right to access non-copyrighted works in the public domain, because the DMCA permits authors to use access and copy controls to protect non-copyrighted works and copyrighted works alike. *See*, *e.g., 321 Studios*, 307 F. Supp. 2d at 1102; *Elcom*, 203 F. Supp. 2d at 1134. Neither the DMCA nor the presence of access or copy controls affect whether or not a work is in the public domain. *321 Studios*, 307 F. Supp. 2d at 1102.

V.D. Penalties

For the first criminal violation of Title I of the DMCA (§§ 1201, 1202), the maximum penalty is five years' imprisonment, a $500,000 fine, or both. 17 U.S.C. § 1204. For subsequent offenses, each of those punishments can be doubled. *Id.* For a more complete discussion of sentencing issues, see Chapter VIII of this Manual.