Copyright 4: Anticircumvention, Tech Mandates, and "Trusted" Systems
- *DMCA Anticircumvention*, 17 U.S.C. 1201
- *Universal v. Corley*, 273 F.3d. 429, (2d Cir. 2001)
- *Lexmark v. Static Control Components*, 387 F.3d 522 (6th Cir. 2005)
- Wendy Seltzer, *The Broadcast Flag: It's not just TV*, 57 Fed. Comm. L.J. 209 (2005), <http://www.law.indiana.edu/fclj/pubs/v57/no2/Seltzer.pdf>

For further reading (optional):
- Julie Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" In Cyberspace*" 28 Conn. L. Rev 981 (1996), <http://cyber.law.harvard.edu/property/alternative/Cohen.html>
- Pam Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, BTLJ (1999), <http://www.sims.berkeley.edu/%7Epam/papers/Samuelson_IP_dig_eco_htm.htm>
- Fred von Lohmann, *Measuring the DMCA Against the Darknet*, 24 Loyola of Los Angeles L.Rev. 635 (2005) <http://www.eff.org/IP/DMCA/DMCA_against_the_darknet.pdf>
- EFF, *Unintended Consequences* <http://www.eff.org/IP/DMCA/unintended_consequences.php>
- Dean Marks and Bruce Turnbull, *Technical Protection Measures: The intersection of technology, law and commercial licenses*, 46 J. Copyright Soc'y U.S. 563 (1999), <http://www.wipo.org/documents/en/meetings/1999/wct_wppt/doc/imp99_3.doc>

Among the most significant developments in the reach for a new equilibrium in copyright law, the Digital Millennium Copyright Act's anticircumvention provision, § 1201, creates new legal rights around technological protection measures that control access to or copying of copyrighted works. Prof. David Nimmer calls these new anticircumvention rights "paracopyright." 1 Nimmer on Copyright (1999 Supp.), 12A-30. Publishers and entertainment companies argued that these protections were necessary in a digital environment that made copying easier than ever; librarians and computer scientists argued that the provisions would curtail lawful fair use and technological innovation.

The first major battle over these new rights erupted around the digital video disc (DVD), and its CSS encryption. 2600 Magazine posted and linked to DeCSS, computer code capable of decrypting the DVD files. As District Judge Lewis Kaplan, of the Southern District of New York, described the conflict:

> In the final analysis, the dispute between these parties is simply put if not necessarily simply resolved.
>
> Plaintiffs have invested huge sums over the years in producing motion pictures in reliance upon a legal framework that, through the law of copyright, has ensured

that they will have the exclusive right to copy and distribute those motion pictures for economic gain. They contend that the advent of new technology should not alter this long established structure.

Defendants, on the other hand, are adherents of a movement that believes that information should be avail-able without charge to anyone clever enough to break into the computer systems or data storage media in which it is located. Less radically, they have raised a legitimate concern about the possible impact on traditional fair use of access control measures in the digital era.

Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 345-46 (S.D.N.Y. 2000). The Second Circuit upheld his injunction against posting and linking DeCSS in *Universal v. Corley*, as the case was labeled on appeal. Does the *Corley* ruling strike the right balance among copyright, technology, and First Amendment concerns? What about the problem Linux users still face obtaining licensed DVD player software for their operating system?

The DMCA has been invoked to support copy controls on digital movies, music, and e-books. It has also been called in to block the sale of interoperable garage door openers, *Chamberlain Group, Inc. v. Skylink Techs, Inc.*, 381 F.3d 1178 (Fed. Cir. 2004), and replacement print cartridges, *Lexmark v. Static Control Components*, 387 F.3d 522 (6th Cir. 2005). Does the law support these extensions?

Consider this hypothetical:

Life-Time, Inc., distributes free CD-ROMs through a mass mailing campaign. The CD-ROMs contain a huge collection of celebrity photos and interviews. Readers who use the CDs in their computers find that they can sample--i.e. get access to--up to three interviews, selecting from a list. After the user selects and views three interviews, the program offers an 800 number that, when called, allows the user to offer a credit card number and be charged $9.95 for twenty more interviews. After payment is verified, the caller is given an "unlock" code that causes the program to permit viewing of the additional requested interviews.

Jane Doe is sent a copy of the CD, explores it, and thanks to her undergraduate work in computer science is able to crack the CD's protection scheme and view all 2,000 interviews at her leisure without paying for a single one.

Should the law penalize Jane in any way for what she did? Does it?

The DMCA gives legal tools to the copyright holder who employs a "a technological measure that effectively controls" access to or copying of a copyrighted work, but the law specifically does not mandate a particular technological design (apart from requiring Macrovision compliance in analog video recorders). *See* § 1201(c)(3) "Nothing in this section shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure…" In other words, if a copyright

holder has not employed TPMs, technology companies are free to build copying machines. In other places, however, entertainment companies have lobbied for affirmative mandates. Fights over "broadcast flags" for both digital television and digital radio are currently brewing.

In late 2003, the Federal Communications Commission issued a rule requiring all digital television tuners to incorporate government-approved output restrictions designed to prevent redistribution. Among others, advocates of open-source software were concerned that these restrictions were incompatible with open source. The American Library Association led a challenge to the FCC's jurisdiction, and got the Order dismissed by the D.C. Circuit, *Am. Library Ass'n v. FCC*, 401 F.3d. 489 (DC Cir. 2005). As of October 2005, entertainment companies are lobbying Congress for broadcast flag legislation. See <http://www.eff.org/deeplinks/archives/004047.php>

17 U.S.C. § 1201. Circumvention of copyright protection systems

(a) Violations regarding circumvention of technological measures.

  (1) (A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter [enacted Oct. 28, 1998].

    (B) The prohibition contained in subparagraph (A) shall not apply to persons who are users of a copyrighted work which is in a particular class of works, if such persons are, or are likely to be in the succeeding 3-year period, adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works under this title, as determined under subparagraph (C).

    (C) During the 2-year period described in subparagraph (A), and during each succeeding 3-year period, the Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation, shall make the determination in a rulemaking proceeding for purposes of subparagraph (B) of whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition under subparagraph (A) in their ability to make noninfringing uses under this title of a particular class of copyrighted works. In conducting such rulemaking, the Librarian shall examine--

      (i) the availability for use of copyrighted works;

      (ii) the availability for use of works for nonprofit archival, preservation, and educational purposes;

      (iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;

      (iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and

      (v) such other factors as the Librarian considers appropriate.

    (D) The Librarian shall publish any class of copyrighted works for which the Librarian has determined, pursuant to the rulemaking conducted under subparagraph (C), that noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected, and the prohibition contained in subparagraph (A) shall not apply to such users with respect to such class of works for the ensuing 3-year period.

    (E) Neither the exception under subparagraph (B) from the applicability of the prohibition contained in subparagraph (A), nor any determination made in a rulemaking conducted under subparagraph (C), may be used as a defense in any action to enforce any provision of this title other than this paragraph.

  (2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that--

    (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

    (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this

title; or

    (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

  (3) As used in this subsection--

    (A) to "circumvent a technological measure" means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner; and

    (B) a technological measure "effectively controls access to a work" if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.

(b) Additional violations.

  (1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that--

    (A) is primarily designed or produced for the purpose of circumventing 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;

    (B) has only limited commercially significant purpose or use other than to circumvent 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; or

    (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing 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.

  (2) As used in this subsection--

    (A) to "circumvent protection afforded by a technological measure" means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure; and

    (B) 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.

(c) Other rights, etc., not affected.

  (1) Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.

  (2) Nothing in this section shall enlarge or diminish vicarious or contributory liability for copyright infringement in connection with any technology, product, service, device, component, or part thereof.

  (3) Nothing in this section shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure, so long as such part or component, or the product in which such part or component is integrated, does not otherwise fall within the prohibitions of subsection (a)(2) or (b)(1).

  (4) Nothing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products.

(d) Exemption for nonprofit libraries, archives, and educational institutions.

  (1) A nonprofit library, archives, or educational institution which gains access to a commercially exploited copyrighted work solely in order to make a good faith determination of whether to acquire a copy of that work for the sole purpose of engaging in conduct permitted under this title shall not be in violation of subsection (a)(1)(A). A copy of a work to which access has been gained under this paragraph--

    (A) may not be retained longer than necessary to make such good faith determination; and

    (B) may not be used for any other purpose.

  (2) The exemption made available under paragraph (1) shall only apply with respect to a work when an identical copy of that work is not reasonably available in another form.

  (3) A nonprofit library, archives, or educational institution that willfully for the purpose of commercial advantage or financial gain violates paragraph (1)--

    (A) shall, for the first offense, be subject to the civil remedies under section 1203; and

    (B) shall, for repeated or subsequent offenses, in addition to the civil remedies under section 1203, forfeit the exemption provided under paragraph (1).

  (4) This subsection may not be used as a defense to a claim under subsection (a)(2) or (b), nor may this subsection permit a nonprofit library, archives, or educational institution to manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, component, or part thereof, which circumvents a technological measure.

  (5) In order for a library or archives to qualify for the exemption under this subsection, the collections of that library or archives shall be--

    (A) open to the public; or

    (B) available not only to researchers affiliated with the library or archives or with the institution of which it is a part, but also to other persons doing research in a specialized field.

(e) Law enforcement, intelligence, and other government activities. This section does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State. For purposes of this subsection, the term "information security" means activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network.

(f) Reverse engineering.

  (1) Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that 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 the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.

(2) Notwithstanding the provisions of subsections (a)(2) and (b), a person may develop and employ technological means to circumvent a technological measure, or to circumvent protection afforded by a technological measure, in order to enable the identification and analysis under paragraph (1), or for the purpose of enabling interoperability of an independently created computer program with other programs, if such means are necessary to achieve such interoperability, to the extent that doing so does not constitute infringement under this title.

(3) The information acquired through the acts permitted under paragraph (1), and the means permitted under paragraph (2), may be made available to others if the person referred to in paragraph (1) or (2), as the case may be, provides such information or means solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement under this title or violate applicable law other than this section.

(4) For purposes of this subsection, the term "interoperability" means the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged.

(g) Encryption research.
 (1) Definitions. For purposes of this subsection--
   (A) the term "encryption research" means 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; and
   (B) the term "encryption technology" means the scrambling and descrambling of information using mathematical formulas or algorithms.
 (2) Permissible acts of encryption research. Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent 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--
   (A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work;
   (B) such act is necessary to conduct such encryption research;
   (C) the person made a good faith effort to obtain authorization before the circumvention; and
   (D) such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986
 (3) Factors in determining exemption. In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include--
   (A) whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security;
   (B) whether the person is engaged in a legitimate course of study, is employed, or is

appropriately trained or experienced, in the field of encryption technology; and

    (C) whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research, and the time when such notice is provided.

  (4) Use of technological means for research activities. Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to--

    (A) 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 paragraph (2); and

    (B) provide the technological means to another person with whom he or she is working collaboratively for the purpose of conducting the acts of good faith encryption research described in paragraph (2) or for the purpose of having that other person verify his or her acts of good faith encryption research described in paragraph (2).

  (5) Report to Congress. Not later than 1 year after the date of the enactment of this chapter [enacted Oct. 28, 1998], the Register of Copyrights and the Assistant Secretary for Communications and Information of the Department of Commerce shall jointly report to the Congress on the effect this subsection has had on--

    (A) encryption research and the development of encryption technology;

    (B) the adequacy and effectiveness of technological measures designed to protect copyrighted works; and

    (C) protection of copyright owners against the unauthorized access to their encrypted copyrighted works.

  The report shall include legislative recommendations, if any.

(h) Exceptions regarding minors. In applying subsection (a) to a component or part, the court may 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.

(i) Protection of personally identifying information.

  (1) Circumvention permitted. Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure that effectively controls access to a work protected under this title, if--

    (A) the technological measure, or the work it protects, contains the capability of collecting or disseminating personally identifying information reflecting the online activities of a natural person who seeks to gain access to the work protected;

    (B) in the normal course of its operation, the technological measure, or the work it protects, collects or disseminates personally identifying information about the person who seeks to gain access to the work protected, without providing conspicuous notice of such collection or dissemination to such person, and without providing such person with the capability to prevent or restrict such collection or dissemination;

    (C) the act of circumvention has the sole effect of identifying and disabling the capability described in subparagraph (A), and has no other effect on the ability of any person to gain access to any work; and

    (D) the act of circumvention is carried out solely for the purpose of preventing the

collection or dissemination of personally identifying information about a natural person who seeks to gain access to the work protected, and is not in violation of any other law.

   (2) Inapplicability to certain technological measures. This subsection does not apply to a technological measure, or a work it protects, that does not collect or disseminate personally identifying information and that is disclosed to a user as not having or using such capability.

(j) Security testing.
   (1) Definition. For purposes of this subsection, the term "security testing" means 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.
   (2) Permissible acts of security testing. Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to engage in an act of security testing, if such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.
   (3) Factors in determining exemption. In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include--
      (A) whether the information derived from the security testing was used solely to promote the security of the owner or operator of such computer, computer system or computer network, or shared directly with the developer of such computer, computer system, or computer network; and
      (B) whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security.
   (4) Use of technological means for security testing. Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to develop, produce, distribute or employ technological means for the sole purpose of performing the acts of security testing described in subsection (2) [subsection (a)(2)], provided such technological means does not otherwise violate section (a)(2).

(k) Certain analog devices and certain technological measures.
   (1) Certain analog devices.
      (A) Effective 18 months after the date of the enactment of this chapter [enacted Oct. 28, 1998], no person shall manufacture, import, offer to the public, provide or otherwise traffic in any--
         (i) VHS format analog video cassette recorder unless such recorder conforms to the automatic gain control copy control technology;
         (ii) 8mm format analog video cassette camcorder unless such camcorder conforms to the automatic gain control technology;
         (iii) Beta format analog video cassette recorder, unless such recorder conforms to the automatic gain control copy control technology, except that this requirement shall not apply until there are 1,000 Beta format analog video cassette recorders sold in the United

States in any one calendar year after the date of the enactment of this chapter [enacted Oct. 28, 1998];

(iv) 8mm format analog video cassette recorder that is not an analog video cassette camcorder, unless such recorder conforms to the automatic gain control copy control technology, except that this requirement shall not apply until there are 20,000 such recorders sold in the United States in any one calendar year after the date of the enactment of this chapter [enacted Oct. 28, 1998]; or

(v) analog video cassette recorder that records using an NTSC format video input and that is not otherwise covered under clauses (i) through (iv), unless such device conforms to the automatic gain control copy control technology.

(B) Effective on the date of the enactment of this chapter [enacted Oct. 28, 1998], no person shall manufacture, import, offer to the public, provide or otherwise traffic in--

(i) any VHS format analog video cassette recorder or any 8mm format analog video cassette recorder if the design of the model of such recorder has been modified after such date of enactment so that a model of recorder that previously conformed to the automatic gain control copy control technology no longer conforms to such technology; or

(ii) any VHS format analog video cassette recorder, or any 8mm format analog video cassette recorder that is not an 8mm analog video cassette camcorder, if the design of the model of such recorder has been modified after such date of enactment so that a model of recorder that previously conformed to the four-line colorstripe copy control technology no longer conforms to such technology.

Manufacturers that have not previously manufactured or sold a VHS format analog video cassette recorder, or an 8mm format analog cassette recorder, shall be required to conform to the four-line colorstripe copy control technology in the initial model of any such recorder manufactured after the date of the enactment of this chapter [enacted Oct. 28, 1998], and thereafter to continue conforming to the four-line colorstripe copy control technology. For purposes of this subparagraph, an analog video cassette recorder "conforms to" the four-line colorstripe copy control technology if it records a signal that, when played back by the playback function of that recorder in the normal viewing mode, exhibits, on a reference display device, a display containing distracting visible lines through portions of the viewable picture.

 (2) Certain encoding restrictions. No person shall apply the automatic gain control copy control technology or colorstripe copy control technology to prevent or limit consumer copying except such copying--

(A) of a single transmission, or specified group of transmissions, of live events or of audiovisual works for which a member of the public has exercised choice in selecting the transmissions, including the content of the transmissions or the time of receipt of such transmissions, or both, and as to which such member is charged a separate fee for each such transmission or specified group of transmissions;

(B) from a copy of a transmission of a live event or an audiovisual work if such transmission is provided by a channel or service where payment is made by a member of the public for such channel or service in the form of a subscription fee that entitles the member of the public to receive all of the programming contained in such channel or service;

(C) from a physical medium containing one or more prerecorded audiovisual works; or

(D) from a copy of a transmission described in subparagraph (A) or from a copy made from a physical medium described in subparagraph (C).

In the event that a transmission meets both the conditions set forth in subparagraph (A) and those set forth in subparagraph (B), the transmission shall be treated as a transmission described in subparagraph (A).

(3) Inapplicability. This subsection shall not--

(A) require any analog video cassette camcorder to conform to the automatic gain control copy control technology with respect to any video signal received through a camera lens;

(B) apply to the manufacture, importation, offer for sale, provision of, or other trafficking in, any professional analog video cassette recorder; or

(C) apply to the offer for sale or provision of, or other trafficking in, any previously owned analog video cassette recorder, if such recorder was legally manufactured and sold when new and not subsequently modified in violation of paragraph (1)(B).

(4) Definitions. For purposes of this subsection:

(A) An "analog video cassette recorder" means a device that records, or a device that includes a function that records, on electromagnetic tape in an analog format the electronic impulses produced by the video and audio portions of a television program, motion picture, or other form of audiovisual work.

(B) An "analog video cassette camcorder" means an analog video cassette recorder that contains a recording function that operates through a camera lens and through a video input that may be connected with a television or other video playback device.

(C) An analog video cassette recorder "conforms" to the automatic gain control copy control technology if it--

(i) detects one or more of the elements of such technology and does not record the motion picture or transmission protected by such technology; or

(ii) records a signal that, when played back, exhibits a meaningfully distorted or degraded display.

(D) The term "professional analog video cassette recorder" means an analog video cassette recorder that is designed, manufactured, marketed, and intended for use by a person who regularly employs such a device for a lawful business or industrial use, including making, performing, displaying, distributing, or transmitting copies of motion pictures on a commercial scale.

(E) The terms " VHS format", "8mm format", "Beta format", "automatic gain control copy control technology", "colorstripe copy control technology", "four-line version of the colorstripe copy control technology", and "NTSC" have the meanings that are commonly understood in the consumer electronics and motion picture industries as of the date of the enactment of this chapter [enacted Oct. 28, 1998].

(5) Violations. Any violation of paragraph (1) of this subsection shall be treated as a violation of subsection (b)(1) of this section. Any violation of paragraph (2) of this subsection shall be deemed an "act of circumvention" for the purposes of section 1203(c)(3)(A) of this chapter.

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

JON O. NEWMAN, Circuit Judge.

When the Framers of the First Amendment prohibited Congress from making any law "abridging the freedom of speech," they were not thinking about computers, computer programs, or the Internet. But neither were they thinking about radio, television, or movies. Just as the inventions at the beginning and middle of the 20th century presented new First Amendment issues, so does the cyber revolution at the end of that century. This appeal raises significant First Amendment issues concerning one aspect of computer technology--encryption to protect materials in digital form from unauthorized access. The appeal challenges the constitutionality of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201 et seq. (Supp. V 1999) and the validity of an injunction entered to enforce the DMCA.

Defendant-Appellant Eric C. Corley and his company, 2600 Enterprises, Inc., (collectively "Corley," "the Defendants,"or "the Appellants") appeal from the amended final judgment of the United States District Court for the Southern District of New York (Lewis A. Kaplan, District Judge), entered August 23, 2000, enjoining them from various actions concerning a decryption program known as "DeCSS." Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 346 (S.D.N.Y. 2000) ("Universal II"). The injunction primarily bars the Appellants from posting DeCSS on their web site and from knowingly linking their web site to any other web site on which DeCSS is posted. We affirm.

…This appeal concerns the anti-trafficking provisions of the DMCA, which Congress enacted in 1998 to strengthen copyright protection in the digital age. Fearful that the ease with which pirates could copy and distribute a copyrightable work in digital form was overwhelming the capacity of conventional copyright enforcement to find and enjoin unlawfully copied material, Congress sought to combat copyright piracy in its earlier stages, before the work was even copied. The DMCA therefore backed with legal sanctions the efforts of copyright owners to protect their works from piracy behind digital walls such as encryption codes or password protections. In so doing, Congress targeted not only those pirates who would circumvent these digital walls (the "anti-circumvention provisions," contained in 17 U.S.C. § 1201 (a)(1)), but also anyone who would traffic in a technology primarily designed to circumvent a digital wall (the "anti-trafficking provisions," contained in 17 U.S.C. § 1201 (a)(2), (b)(1)).

Corley publishes a print magazine and maintains an affiliated web site geared towards "hackers," a digital-era term often applied to those interested in techniques for circumventing protections of computers and computer data from unauthorized access. The so-called hacker community includes serious computer-science scholars conducting research on protection techniques, computer buffs intrigued by the challenge of trying to circumvent access-limiting devices or perhaps hoping to promote security by exposing flaws in protection techniques, mischief-makers interested in disrupting computer operations, and thieves, including copyright infringers who want to acquire copyrighted

material (for personal use or resale) without paying for it.

In November 1999, Corley posted a copy of the decryption computer program "DeCSS" on his web site, http://www.2600.com ("2600.com"). DeCSS is designed to circumvent "CSS," the encryption technology that motion picture studios place on DVDs to prevent the unauthorized viewing and copying of motion pictures. Corley also posted on his web site links to other web sites where DeCSS could be found.

Plaintiffs-Appellees are eight motion picture studios that brought an action in the Southern District of New York seeking injunctive relief against Corley under the DMCA. Following a full non-jury trial, the District Court entered a permanent injunction barring Corley from posting DeCSS on his web site or from knowingly linking via a hyperlink to any other web site containing DeCSS. The District Court rejected Corley's constitutional attacks on the statute and the injunction.

Corley renews his constitutional challenges on appeal. Specifically, he argues primarily that: (1) the DMCA oversteps limits in the Copyright Clause on the duration of copyright protection; (2) the DMCA as applied to his dissemination of DeCSS violates the First Amendment because computer code is "speech" entitled to full First Amendment protection and the DMCA fails to survive the exacting scrutiny accorded statutes that regulate "speech"; and (3) the DMCA violates the First Amendment and the Copyright Clause by unduly obstructing the "fair use" of copyrighted materials. Corley also argues that the statute is susceptible to, and should therefore be given, a narrow interpretation that avoids alleged constitutional objections.

Background
…In the early 1990s, the studios began to consider the possibility of distributing movies in digital form…. Movies in digital form are placed on disks, known as DVDs, which can be played on a DVD player (either a stand-alone device or a component of a computer). DVDs offer advantages over analog tapes, such as improved visual and audio quality, larger data capacity, and greater durability. However, the improved quality of a movie in a digital format brings with it the risk that a virtually perfect copy, i.e., one that will not lose perceptible quality in the copying process, can be readily made at the click of a computer control and instantly distributed to countless recipients throughout the world over the Internet. …

I. CSS

The movie studios were reluctant to release movies in digital form until they were confident they had in place adequate safeguards against piracy of their copyrighted movies. The studios took several steps to minimize the piracy threat. First, they settled on the DVD as the standard digital medium for home distribution of movies. The studios then sought an encryption scheme to protect movies on DVDs. They enlisted the help of members of the consumer electronics and computer industries, who in mid-1996 developed the Content Scramble System ("CSS"). CSS is an encryption scheme that employs an algorithm configured by a set of "keys" to encrypt a DVD's contents. The

algorithm is a type of mathematical formula for transforming the contents of the movie file into gibberish; the "keys" are in actuality strings of 0's and 1's that serve as values for the mathematical formula. Decryption in the case of CSS requires a set of "player keys" contained in compliant DVD players, as well as an understanding of the CSS encryption algorithm. Without the player keys and the algorithm, a DVD player cannot access the contents of a DVD. With the player keys and the algorithm, a DVD player 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 of the DVD.

The studios developed a licensing scheme for distributing the technology to manufacturers of DVD players. Player keys and other information necessary to the CSS scheme were given to manufacturers of DVD players for an administrative fee. In exchange for the licenses, manufacturers were obliged to keep the player keys confidential. Manufacturers were also required in the licensing agreement to prevent the transmission of "CSS data" (a term undefined in the licensing agreement) from a DVD drive to any "internal recording device," including, presumably, a computer hard drive….

 II. DeCSS

In September 1999, Jon Johansen, a Norwegian teenager, collaborating with two unidentified individuals he met on the Internet, reverse-engineered a licensed DVD player designed to operate on the Microsoft operating system, and culled from it the player keys and other information necessary to decrypt CSS. The record suggests that Johansen was trying to develop a DVD player operable on Linux, an alternative operating system that did not support any licensed DVD players at that time. In order to accomplish this task, Johansen wrote a decryption program executable on Microsoft's operating system. That program was called, appropriately enough, "DeCSS."

If a user runs the DeCSS program (for example, by clicking on the DeCSS icon on a Microsoft operating system platform) with a DVD in the computer's disk drive, DeCSS will decrypt the DVD's CSS protection, allowing the user to copy the DVD's files and place the copy on the user's hard drive. The result is a very large computer file that can be played on a non-CSS-compliant player and copied, manipulated, and transferred just like any other computer file. n5 DeCSS comes complete with a fairly user-friendly interface that helps the user select from among the DVD's files and assign the decrypted file a location on the user's hard drive. The quality of the resulting decrypted movie is "virtually identical" to that of the encrypted movie on the DVD. And the file produced by DeCSS, while large, can be compressed to a manageable size by a compression software called "DivX," available at no cost on the Internet. This compressed file can be copied onto a DVD, or transferred over the Internet (with some patience).

Johansen posted the executable object code, but not the source code, for DeCSS on his web site. The distinction between source code and object code is relevant to this case, so a brief explanation is warranted. A computer responds to electrical charges, the presence or absence of which is represented by strings of 1's and 0's. Strictly speaking, "object

14

code" consists of those 1's and 0's. While some people can read and program in object code, "it would be inconvenient, inefficient and, for most people, probably impossible to do so." Computer languages have been written to facilitate program writing and reading. A program in such a computer language--BASIC, C, and Java are examples--is said to be written in "source code." Source code has the benefit of being much easier to read (by people) than object code, but as a general matter, it must be translated back to object code before it can be read by a computer….

In November 1999, Corley wrote and placed on his web site, 2600.com, an article about the DeCSS phenomenon. His web site is an auxiliary to the print magazine, 2600: The Hacker Quarterly, which Corley has been publishing since 1984. As the name suggests, the magazine is designed for "hackers," as is the web site. While the magazine and the web site cover some issues of general interest to computer users--such as threats to online privacy--the focus of the publications is on the vulnerability of computer security systems, and more specifically, how to exploit that vulnerability in order to circumvent the security systems. Representative articles explain how to steal an Internet domain name and how to break into the computer systems at Federal Express.

Corley's article about DeCSS detailed how CSS was cracked, and described the movie industry's efforts to shut down web sites posting DeCSS. It also explained that DeCSS could be used to copy DVDs. At the end of the article, the Defendants posted copies of the object and source code of DeCSS. In Corley's words, he added the code to the story because "in a journalistic world, . . . you have to show your evidence . . . and particularly in the magazine that I work for, people want to see specifically what it is that we are referring to," including "what evidence . . . we have" that there is in fact technology that circumvents CSS. Writing about DeCSS without including the DeCSS code would have been, to Corley, "analogous to printing a story about a picture and not printing the picture." Corley also added to the article links that he explained would take the reader to other web sites where DeCSS could be found.

2600.com was only one of hundreds of web sites that began posting DeCSS near the end of 1999. The movie industry tried to stem the tide by sending cease-and-desist letters to many of these sites. These efforts met with only partial success; a number of sites refused to remove DeCSS. In January 2000, the studios filed this lawsuit.

III. The DMCA

The DMCA was enacted in 1998 to implement the World Intellectual Property Organization Copyright Treaty ("WIPO Treaty"), which requires contracting parties to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law." Even before the treaty, Congress had been devoting attention to the problems faced by copyright enforcement in the digital age. Hearings on the topic have spanned several years. This legislative effort resulted in the DMCA.

The Act contains three provisions targeted at the circumvention of technological protections. The first is subsection 1201(a)(1)(A), the anti-circumvention provision. n9 This provision prohibits a person from "circumventing a technological measure that effectively controls access to a work protected under [Title 17, governing copyright]." The Librarian of Congress is required to promulgate regulations every three years exempting from this subsection individuals who would otherwise be "adversely affected" in "their ability to make noninfringing uses." 17 U.S.C. § 1201 (a)(1)(B)-(E).

The second and third provisions are subsections 1201(a)(2) and 1201(b)(1), the "anti-trafficking provisions." Subsection 1201(a)(2), the provision at issue in this case, provides:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that--
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
>
> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

Id. § 1201(a)(2). To "circumvent a technological measure" is defined, in pertinent part, as "to descramble a scrambled work . . . or otherwise to . . . bypass . . . a technological measure, without the authority of the copyright owner." Id. § 1201(a)(3)(A).

Subsection 1201(b)(1) is similar to subsection 1201(a)(2), except that subsection 1201(a)(2) covers those who traffic in technology that can circumvent "a technological measure that effectively controls access to a work protected under" Title 17, whereas subsection 1201(b)(1) covers those who traffic in technology that can circumvent "protection afforded by a technological measure that effectively protects a right of a copyright owner under" Title 17. Id. § 1201(a)(2), (b)(1) (emphases added). In other words, although both subsections prohibit trafficking in a circumvention technology, the focus of subsection 1201(a)(2) is circumvention of technologies designed to prevent access to a work, and the focus of subsection 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. Subsection 1201(a)(1) differs from both of these anti-trafficking subsections in that it targets the use of a circumvention technology, not the trafficking in such a technology.

The DMCA contains exceptions for schools and libraries that want to use circumvention technologies to determine whether to purchase a copyrighted product, [17 U.S.C. § 1201](d); individuals using circumvention technology "for the sole purpose" of trying to achieve "interoperability" of computer programs through reverse-engineering, id. § 1201(f); encryption research aimed at identifying flaws in encryption technology, if the research is conducted to advance the state of knowledge in the field, id. § 1201(g); and several other exceptions not relevant here.

The DMCA creates civil remedies, id. § 1203, and criminal sanctions, id. § 1204. It specifically authorizes a court to "grant temporary and permanent injunctions on such terms as it deems reasonable to prevent or restrain a violation." Id. § 1203(b)(1).

IV. Procedural History

Invoking subsection 1203(b)(1), the Plaintiffs sought an injunction against the Defendants, alleging that the Defendants violated the anti-trafficking provisions of the statute. On January 20, 2000, after a hearing, the District Court issued a preliminary injunction barring the Defendants from posting DeCSS.

The Defendants complied with the preliminary injunction, but continued to post links to other web sites carrying DeCSS, an action they termed "electronic civil disobedience." Under the heading "Stop the MPAA [(Motion Picture Association of America)]," Corley urged other web sites to post DeCSS lest "we . . . be forced into submission."

The Plaintiffs then sought a permanent injunction barring the Defendants from both posting DeCSS and linking to sites containing DeCSS. After a trial on the merits, the Court issued a comprehensive opinion, Universal I, and granted a permanent injunction, Universal II….

The Court's injunction barred the Defendants from: "posting on any Internet web site" DeCSS; "in any other way . . . offering to the public, providing, or otherwise trafficking in DeCSS"; violating the anti-trafficking provisions of the DMCA in any other manner, and finally "knowingly linking any Internet web site operated by them to any other web site containing DeCSS, or knowingly maintaining any such link, for the purpose of disseminating DeCSS." …

 Discussion

I. Narrow Construction to Avoid Constitutional Doubt

The Appellants first argue that, because their constitutional arguments are at least substantial, we should interpret the statute narrowly so as to avoid constitutional problems. [T]he Appellants argue that an individual who buys a DVD has the "authority of the copyright owner" to view the DVD, and therefore is exempted from the DMCA pursuant to subsection 1201(a)(3)(A) when the buyer circumvents an encryption

technology in order to view the DVD on a competing platform (such as Linux). The basic flaw in this argument is that it misreads subsection 1201(a)(3)(A). That provision exempts from liability those who would "decrypt" an encrypted DVD with the authority of a copyright owner, not those who would "view" a DVD with the authority of a copyright owner. In any event, the Defendants offered no evidence that the Plaintiffs have either explicitly or implicitly authorized DVD buyers to circumvent encryption technology to support use on multiple platforms.

…

III. Constitutional Challenges Based on the First Amendment

[Next, to resolve the Appellants' First Amendment challenges, we consider] whether computer code is speech, whether computer programs are speech, the scope of First Amendment protection for computer code, and the scope of First Amendment protection for decryption code. Based on our analysis of these issues, we then consider the Appellants' challenge to the injunction's provisions concerning posting and linking.

1. Code as Speech

Communication does not lose constitutional protection as "speech" simply because it is expressed in the language of computer code. Mathematical formulae and musical scores are written in "code," i.e., symbolic notations not comprehensible to the uninitiated, and yet both are covered by the First Amendment. If someone chose to write a novel entirely in computer object code by using strings of 1's and 0's for each letter of each word, the resulting work would be no different for constitutional purposes than if it had been written in English. The "object code" version would be incomprehensible to readers outside the programming community (and tedious to read even for most within the community), but it would be no more incomprehensible than a work written in Sanskrit for those unversed in that language. The undisputed evidence reveals that even pure object code can be, and often is, read and understood by experienced programmers. And source code (in any of its various levels of complexity) can be read by many more. See Universal I, 111 F. Supp. 2d at 326. Ultimately, however, the ease with which a work is comprehended is irrelevant to the constitutional inquiry. If computer code is distinguishable from conventional speech for First Amendment purposes, it is not because it is written in an obscure language. See Junger v. Daley, 209 F.3d 481, 484 (6th Cir. 2000).

2. Computer Programs as Speech

Of course, computer code is not likely to be the language in which a work of literature is written. Instead, it is primarily the language for programs executable by a computer. These programs are essentially instructions to a computer. In general, programs may give instructions either to perform a task or series of tasks when initiated by a single (or double) click of a mouse or, once a program is operational ("launched"), to manipulate data that the user enters into the computer. Whether computer code that gives a computer instructions is "speech" within the meaning of the First Amendment requires

18

consideration of the scope of the Constitution's protection of speech.

The First Amendment provides that "Congress shall make no law . . . abridging the freedom of speech . . . ." U.S. Const. amend. I. "Speech" is an elusive term, and judges and scholars have debated its bounds for two centuries. …

Thus, for example, courts have subjected to First Amendment scrutiny restrictions on the dissemination of technical scientific information, United States v. Progressive, Inc., 467 F. Supp. 990 (W.D. Wis. 1979), and scientific research, Stanford University, 773 F. Supp. at 473, and attempts to regulate the publication of instructions, see, e.g., United States v. Raymond, 228 F.3d 804, 815 (7th Cir. 2000) (First Amendment does not protect instructions for violating the tax laws); United States v. Dahlstrom, 713 F.2d 1423, 1428 (9th Cir. 1983) (same); Herceg v. Hustler Magazine, Inc., 814 F.2d 1017, 1020-25 (5th Cir. 1987) (First Amendment protects instructions for engaging in a dangerous sex act)…

Computer programs are not exempted from the category of First Amendment speech simply because their instructions require use of a computer. A recipe is no less "speech" because it calls for the use of an oven, and a musical score is no less "speech" because it specifies performance on an electric guitar. Arguably distinguishing computer programs from conventional language instructions is the fact that programs are executable on a computer. But the fact that a program has the capacity to direct the functioning of a computer does not mean that it lacks the additional capacity to convey information, and it is the conveying of information that renders instructions "speech" for purposes of the First Amendment. The information conveyed by most "instructions" is how to perform a task.

Instructions such as computer code, which are intended to be executable by a computer, will often convey information capable of comprehension and assessment by a human being. A programmer reading a program learns information about instructing a computer, and might use this information to improve personal programming skills and perhaps the craft of programming. Moreover, programmers communicating ideas to one another almost inevitably communicate in code, much as musicians use notes. Limiting First Amendment protection of programmers to descriptions of computer code (but not the code itself) would impede discourse among computer scholars, just as limiting protection for musicians to descriptions of musical scores (but not sequences of notes) would impede their exchange of ideas and expression. Instructions that communicate information comprehensible to a human qualify as speech whether the instructions are designed for execution by a computer or a human (or both).

Vartuli is not to the contrary. The defendants in *Vartuli* marketed a software program called "Recurrence," which would tell computer users when to buy or sell currency futures contracts if their computers were fed currency market rates. The Commodity Futures Trading Commission charged the defendants with violating federal law for, among other things, failing to register as commodity trading advisors for their distribution of the Recurrence software. The defendants maintained that Recurrence's cues to users to buy or sell were protected speech, and that the registration requirement as

19

applied to Recurrence was a constitutionally suspect prior restraint. We rejected the defendants' constitutional claim, holding that Recurrence "in the form it was sold and marketed by the defendants" did not generate speech protected by the First Amendment. Vartuli, 228 F.3d at 111.

Essential to our ruling in *Vartuli* was the manner in which the defendants marketed the software and intended that it be used: the defendants told users of the software to follow the software's cues "with no second-guessing," id., and intended that users follow Recurrence's commands "mechanically" and "without the intercession of the mind or the will of the recipient," id. We held that the values served by the First Amendment were not advanced by these instructions, even though the instructions were expressed in words. *Id.* We acknowledged that some users would, despite the defendants' marketing, refuse to follow Recurrence's cues mechanically but instead would use the commands as a source of information and advice, and that, as to these users, Recurrence's cues might very "well have been 'speech.'" Id. at 111-12. Nevertheless, we concluded that the Government could require registration for Recurrence's intended use because such use was devoid of any constitutionally protected speech. Id. at 112. …

For all of these reasons, we join the other courts that have concluded that computer code, and computer programs constructed from code, can merit First Amendment protection, see Junger, 209 F.3d at 484; Bernstein, 922 F. Supp. at 1434-36; see also Bernstein, 176 F.3d at 1140-41; Karn v. United States Department of State, 925 F. Supp. 1, 9-10 (D.D.C. 1996) (assuming, without deciding, that source code with English comments interspersed throughout is "speech"), although the scope of such protection remains to be determined.

3. The Scope of First Amendment Protection for Computer Code

Having concluded that computer code conveying information is "speech" within the meaning of the First Amendment, we next consider, to a limited extent, the scope of the protection that code enjoys. As the District Court recognized, the scope of protection for speech generally depends on whether the restriction is imposed because of the content of the speech. Content-based restrictions are permissible only if they serve compelling state interests and do so by the least restrictive means available. …
…

To determine whether regulation of computer code is content-neutral, the initial inquiry must be whether the regulated activity is "sufficiently imbued with elements of communication to fall within the scope of the First . . . Amendment[]." Id. 418 U.S. at 409; see also Name.Space, 202 F.3d at 585. Computer code, as we have noted, often conveys information comprehensible to human beings, even as it also directs a computer to perform various functions. Once a speech component is identified, the inquiry then proceeds to whether the regulation is "justified without reference to the content of regulated speech." Hill, 530 U.S. at 720.

The Appellants vigorously reject the idea that computer code can be regulated according to any different standard than that applicable to pure speech, i.e., speech that lacks a

nonspeech component. Although recognizing that code is a series of instructions to a computer, they argue that code is no different, for First Amendment purposes, than blueprints that instruct an engineer or recipes that instruct a cook. We disagree. Unlike a blueprint or a recipe, which cannot yield any functional result without human comprehension of its content, human decision-making, and human action, computer code can instantly cause a computer to accomplish tasks and instantly render the results of those tasks available throughout the world via the Internet. The only human action required to achieve these results can be as limited and instantaneous as a single click of a mouse. These realities of what code is and what its normal functions are require a First Amendment analysis that treats code as combining nonspeech and speech elements, i.e., functional and expressive elements. See Red Lion Broadcasting Co. v. FCC, 395 U.S. 367, 386 (1969) ("Differences in the characteristics of new media justify differences in the First Amendment standards applied to them.").

We recognize, as did Judge Kaplan, that the functional capability of computer code cannot yield a result until a human being decides to insert the disk containing the code into a computer and causes it to perform its function (or programs a computer to cause the code to perform its function). Nevertheless, this momentary intercession of human action does not diminish the nonspeech component of code, nor render code entirely speech, like a blueprint or a recipe. Judge Kaplan, in a passage that merits extensive quotation, cogently explained why this is especially so with respect to decryption code:

> The focus on functionality in order to determine the level of scrutiny is not an inevitable consequence of the speech-conduct distinction. Conduct has immediate effects on the environment. Computer code, on the other hand, no matter how functional, causes a computer to perform the intended operations only if someone uses the code to do so. Hence, one commentator, in a thoughtful article, has maintained that functionality is really "a proxy for effects or harm" and that its adoption as a determinant of the level of scrutiny slides over questions of causation that intervene between the dissemination of a computer program and any harm caused by its use.

> The characterization of functionality as a proxy for the consequences of use is accurate. But the assumption that the chain of causation is too attenuated to justify the use of functionality to determine the level of scrutiny, at least in this context, is not.

> Society increasingly depends upon technological means of controlling access to digital files and systems, whether they are military computers, bank records, academic records, copyrighted works or something else entirely. There are far too many who, given any opportunity, will bypass security measures, some for the sheer joy of doing it, some for innocuous reasons, and others for more malevolent purposes. Given the virtually instantaneous and worldwide dissemination widely available via the Internet, the only rational assumption is that once a computer program capable of bypassing such an access control system is disseminated, it

will be used. And that is not all.

There was a time when copyright infringement could be dealt with quite adequately by focusing on the infringing act. If someone wished to make and sell high quality but unauthorized copies of a copyrighted book, for example, the infringer needed a printing press. The copyright holder, once aware of the appearance of infringing copies, usually was able to trace the copies up the chain of distribution, find and prosecute the infringer, and shut off the infringement at the source.

In principle, the digital world is very different. Once a decryption program like DeCSS is written, it quickly can be sent all over the world. Every recipient is capable not only of decrypting and perfectly copying plaintiffs' copyrighted DVDs, but also of retransmitting perfect copies of DeCSS and thus enabling every recipient to do the same. They likewise are capable of transmitting perfect copies of the decrypted DVD. The process potentially is exponential rather than linear.

. . .

These considerations drastically alter consideration of the causal link between dissemination of computer programs such as this and their illicit use. Causation in the law ultimately involves practical policy judgments. Here, dissemination itself carries very substantial risk of imminent harm because the mechanism is so unusual by which dissemination of means of circumventing access controls to copyrighted works threatens to produce virtually unstoppable infringement of copyright. In consequence, the causal link between the dissemination of circumvention computer programs and their improper use is more than sufficiently close to warrant selection of a level of constitutional scrutiny based on the programs' functionality.

Universal I, 111 F. Supp. 2d at 331-32. The functionality of computer code properly affects the scope of its First Amendment protection.

4. The Scope of First Amendment Protection for Decryption Code

In considering the scope of First Amendment protection for a decryption program like DeCSS, we must recognize that the essential purpose of encryption code is to prevent unauthorized access. Owners of all property rights are entitled to prohibit access to their property by unauthorized persons. Homeowners can install locks on the doors of their houses. Custodians of valuables can place them in safes. Stores can attach to products security devices that will activate alarms if the products are taken away without purchase. These and similar security devices can be circumvented. Burglars can use skeleton keys to open door locks. Thieves can obtain the combinations to safes. Product security devices can be neutralized.

22

Our case concerns a security device, CSS computer code, that prevents access by unauthorized persons to DVD movies. The CSS code is embedded in the DVD movie. Access to the movie cannot be obtained unless a person has a device, a licensed DVD player, equipped with computer code capable of decrypting the CSS encryption code. In its basic function, CSS is like a lock on a homeowner's door, a combination of a safe, or a security device attached to a store's products.

DeCSS is computer code that can decrypt CSS. In its basic function, it is like a skeleton key that can open a locked door, a combination that can open a safe, or a device that can neutralize the security device attached to a store's products. [FN: More dramatically, the Government calls DeCSS "a digital crowbar."] DeCSS enables anyone to gain access to a DVD movie without using a DVD player.

The initial use of DeCSS to gain access to a DVD movie creates no loss to movie producers because the initial user must purchase the DVD. However, once the DVD is purchased, DeCSS enables the initial user to copy the movie in digital form and transmit it instantly in virtually limitless quantity, thereby depriving the movie producer of sales. The advent of the Internet creates the potential for instantaneous worldwide distribution of the copied material.

At first glance, one might think that Congress has as much authority to regulate the distribution of computer code to decrypt DVD movies as it has to regulate distribution of skeleton keys, combinations to safes, or devices to neutralize store product security devices. However, despite the evident legitimacy of protection against unauthorized access to DVD movies, just like any other property, regulation of decryption code like DeCSS is challenged in this case because DeCSS differs from a skeleton key in one important respect: it not only is capable of performing the function of unlocking the encrypted DVD movie, it also is a form of communication, albeit written in a language not understood by the general public. As a communication, the DeCSS code has a claim to being "speech," and as "speech," it has a claim to being protected by the First Amendment. But just as the realities of what any computer code can accomplish must inform the scope of its constitutional protection, so the capacity of a decryption program like DeCSS to accomplish unauthorized--indeed, unlawful--access to materials in which the Plaintiffs have intellectual property rights must inform and limit the scope of its First Amendment protection. Cf. Red Lion, 395 U.S. at 386 ("Differences in the characteristics of new media justify differences in the First Amendment standards applied to them.").

With all of the foregoing considerations in mind, we next consider the Appellants' First Amendment challenge to the DMCA as applied in the specific prohibitions that have been imposed by the District Court's injunction.

B. First Amendment Challenge

The District Court's injunction applies the DMCA to the Defendants by imposing two types of prohibition, both grounded on the anti-trafficking provisions of the DMCA. The

first prohibits posting DeCSS or any other technology for circumventing CSS on any Internet web site. The second prohibits knowingly linking any Internet web site to any other web site containing DeCSS. The validity of the posting and linking prohibitions must be considered separately.

1. Posting

The initial issue is whether the posting prohibition is content-neutral, since, as we have explained, this classification determines the applicable constitutional standard. … [T]he target of the posting provisions of the injunction--DeCSS--has both a nonspeech and a speech component, and that the DMCA, as applied to the Appellants, and the posting prohibition of the injunction target only the nonspeech component. Neither the DMCA nor the posting prohibition is concerned with whatever capacity DeCSS might have for conveying information to a human being, and that capacity, as previously explained, is what arguably creates a speech component of the decryption code. The DMCA and the posting prohibition are applied to DeCSS solely because of its capacity to instruct a computer to decrypt CSS. That functional capability is not speech within the meaning of the First Amendment. The Government seeks to "justify," Hill, 530 U.S. at 720, both the application of the DMCA and the posting prohibition to the Appellants solely on the basis of the functional capability of DeCSS to instruct a computer to decrypt CSS, i.e., "without reference to the content of the regulated speech," id. This type of regulation is therefore content-neutral, just as would be a restriction on trafficking in skeleton keys identified because of their capacity to unlock jail cells, even though some of the keys happened to bear a slogan or other legend that qualified as a speech component.

As a content-neutral regulation with an incidental effect on a speech component, the regulation must serve a substantial governmental interest, the interest must be unrelated to the suppression of free expression, and the incidental restriction on speech must not burden substantially more speech than is necessary to further that interest. Turner Broadcasting, 512 U.S. at 662. The Government's interest in preventing unauthorized access to encrypted copyrighted material is unquestionably substantial, and the regulation of DeCSS by the posting prohibition plainly serves that interest. Moreover, that interest is unrelated to the suppression of free expression. The injunction regulates the posting of DeCSS, regardless of whether DeCSS code contains any information comprehensible by human beings that would qualify as speech. Whether the incidental regulation on speech burdens substantially more speech than is necessary to further the interest in preventing unauthorized access to copyrighted materials requires some elaboration.

Posting DeCSS on the Appellants' web site makes it instantly available at the click of a mouse to any person in the world with access to the Internet, and such person can then instantly transmit DeCSS to anyone else with Internet access. Although the prohibition on posting prevents the Appellants from conveying to others the speech component of DeCSS, the Appellants have not suggested, much less shown, any technique for barring them from making this instantaneous worldwide distribution of a decryption code that makes a lesser restriction on the code's speech component. It is true that the Government has alternative means of prohibiting unauthorized access to copyrighted materials. For

example, it can create criminal and civil liability for those who gain unauthorized access, and thus it can be argued that the restriction on posting DeCSS is not absolutely necessary to preventing unauthorized access to copyrighted materials. But a content-neutral regulation need not employ the least restrictive means of accomplishing the governmental objective. Id. It need only avoid burdening "substantially more speech than is necessary to further the government's legitimate interests." Id. The prohibition on the Defendants' posting of DeCSS satisfies that standard.

2. Linking

In considering linking, we need to clarify the sense in which the injunction prohibits such activity. Although the injunction defines several terms, it does not define "linking." Nevertheless, it is evident from the District Court's opinion that it is concerned with "hyperlinks," Universal I, 111 F. Supp. 2d at 307; see id. at 339. A hyperlink is a cross-reference (in a distinctive font or color) appearing on one web page that, when activated by the point-and-click of a mouse, brings onto the computer screen another web page. The hyperlink can appear on a screen (window) as text, such as the Internet address ("URL") of the web page being called up or a word or phrase that identifies the web page to be called up, for example, "DeCSS web site." Or the hyperlink can appear as an image, for example, an icon depicting a person sitting at a computer watching a DVD movie and text stating "click here to access DeCSS and see DVD movies for free!" The code for the web page containing the hyperlink includes a computer instruction that associates the link with the URL of the web page to be accessed, such that clicking on the hyperlink instructs the computer to enter the URL of the desired web page and thereby access that page. With a hyperlink on a web page, the linked web site is just one click away.

In applying the DMCA to linking (via hyperlinks), Judge Kaplan recognized, as he had with DeCSS code, that a hyperlink has both a speech and a nonspeech component. It conveys information, the Internet address of the linked web page, and has the functional capacity to bring the content of the linked web page to the user's computer screen. …

To avoid applying the DMCA in a manner that would "burden substantially more speech than is necessary to further the government's legitimate interests," Turner Broadcasting, 512 U.S. at 662, Judge Kaplan adapted the standards of New York Times Co. v. Sullivan, 376 U.S. 254, 283 (1964), to fashion a limited prohibition against linking to web sites containing DeCSS. He required clear and convincing evidence

> that those responsible for the link (a) know at the relevant time that the offending material is on the linked-to site, (b) know that it is circumvention technology that may not lawfully be offered, and (c) create or maintain the link for the purpose of disseminating that technology.

Universal I, 111 F. Supp. 2d at 341. He then found that the evidence satisfied his three-part test by his required standard of proof. Id.

…Under the circumstances amply shown by the record, the injunction's linking

prohibition validly regulates the Appellants' opportunity instantly to enable anyone anywhere to gain unauthorized access to copyrighted movies on DVDs. …

IV. Constitutional Challenge Based on Claimed Restriction of Fair Use

Asserting that fair use "is rooted in and required by both the Copyright Clause and the First Amendment," the Appellants contend that the DMCA, as applied by the District Court, unconstitutionally "eliminates fair use" of copyrighted materials. We reject this extravagant claim.

Preliminarily, we note that the Supreme Court has never held that fair use is constitutionally required, although some isolated statements in its opinions might arguably be enlisted for such a requirement. In Stewart v. Abend, 495 U.S. 207, 109 L. Ed. 2d 184, 110 S. Ct. 1750 (1990), cited by the Appellants, the Court merely noted that fair use "'permits courts to avoid rigid application of the copyright statute when, on occasion, it would stifle the very creativity which that law is designed to foster,'" id. (quoting Iowa State University Research Foundation, Inc. v. American Broadcasting Cos., 621 F.2d 57, 60 (2d Cir. 1980)); see also Harper & Row, Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 560, 85 L. Ed. 2d 588, 105 S. Ct. 2218 (1985) (noting "the First Amendment protections already embodied in the Copyright Act's distinction between copyrightable expression and uncopyrightable facts and ideas, and the latitude for scholarship and comment traditionally afforded by fair use"). In Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 127 L. Ed. 2d 500, 114 S. Ct. 1164 (1994), the Court observed, "From the infancy of copyright protection, some opportunity for fair use of copyrighted materials has been thought necessary to fulfill copyright's very purpose, 'to promote the Progress of Science and useful Arts . . . .'" Id. at 575 (citation omitted); see generally William F. Patry, The Fair Use Privilege in Copyright Law 573-82 (2d ed. 1995) (questioning First Amendment protection for fair use).

We need not explore the extent to which fair use might have constitutional protection, grounded on either the First Amendment or the Copyright Clause, because whatever validity a constitutional claim might have as to an application of the DMCA that impairs fair use of copyrighted materials, such matters are far beyond the scope of this lawsuit for several reasons. In the first place, the Appellants do not claim to be making fair use of any copyrighted materials, and nothing in the injunction prohibits them from making such fair use. They are barred from trafficking in a decryption code that enables unauthorized access to copyrighted materials.

Second, as the District Court properly noted, to whatever extent the anti-trafficking provisions of the DMCA might prevent others from copying portions of DVD movies in order to make fair use of them, "the evidence as to the impact of the anti-trafficking provisions of the DMCA on prospective fair users is scanty and fails adequately to address the issues." Universal I, 111 F. Supp. 2d at 338 n.246.

Third, the Appellants have provided no support for their premise that fair use of DVD movies is constitutionally required to be made by copying the original work in its original

26

format. Their examples of the fair uses that they believe others will be prevented from making all involve copying in a digital format those portions of a DVD movie amenable to fair use, a copying that would enable the fair user to manipulate the digitally copied portions. One example is that of a school child who wishes to copy images from a DVD movie to insert into the student's documentary film. We know of no authority for 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. Although the Appellants insisted at oral argument that they should not be relegated to a "horse and buggy" technique in making fair use of DVD movies, the DMCA does not impose even an arguable limitation on the opportunity to make a variety of traditional fair uses of DVD movies, such as commenting on their content, quoting excerpts from their screenplays, and even recording portions of the video images and sounds on film or tape by pointing a camera, a camcorder, or a microphone at a monitor as it displays the DVD movie. The fact that the resulting copy will not be as perfect or as manipulable as a digital copy obtained by having direct access to the DVD movie in its digital form, provides no basis for a claim of unconstitutional limitation of fair use. A film critic making fair use of a movie by quoting selected lines of dialogue has no constitutionally valid claim that the review (in print or on television) would be technologically superior if the reviewer had not been prevented from using a movie camera in the theater, nor has an art student a valid constitutional claim to fair use of a painting by photographing it in a museum. Fair use has never been held to be a guarantee of access to copyrighted material in order to copy it by the fair user's preferred technique or in the format of the original.

Conclusion

We have considered all the other arguments of the Appellants and conclude that they provide no basis for disturbing the District Court's judgment. Accordingly, the judgment is affirmed.

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

SUTTON, Circuit Judge.

This copyright dispute involves two computer programs, two federal statutes and three theories of liability. The first computer program, known as the "Toner Loading Program," calculates toner level in printers manufactured by Lexmark International. The second computer program, known as the "Printer Engine Program," controls various printer functions on Lexmark printers.

The first statute, the general copyright statute, 17 U.S.C. § 101 *et seq.*, has been with us in one form or another since 1790 and grants copyright protection to "original works of authorship fixed in any tangible medium of expression," *id*. § 102(a), but does not "extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery," *id.* § 102(b). The second federal statute, the Digital Millenium Copyright Act (DMCA), 17 U.S.C. § 1201 *et seq.*, was enacted in 1998 and proscribes the sale of products that may be used to "circumvent a technological measure that effectively controls access to a work" protected by the copyright statute.

These statutes became relevant to these computer programs when Lexmark began selling discount toner cartridges for its printers that only Lexmark could re-fill and that contained a microchip designed to prevent Lexmark printers from functioning with toner cartridges that Lexmark had not re-filled. In an effort to support the market for competing toner cartridges, Static Control Components (SCC) mimicked Lexmark's computer chip and sold it to companies interested in selling remanufactured toner cartridges.

Lexmark brought this action to enjoin the sale of SCC's computer chips and raised three theories of liability in doing so. Lexmark claimed that SCC's chip copied the Toner Loading Program in violation of the federal copyright statute. It claimed that SCC's chip violated the DMCA by circumventing a technological measure designed to control access to the Toner Loading Program. And it claimed that SCC's chip violated the DMCA by circumventing a technological measure designed to control access to the Printer Engine Program.

[The court first analyzed the copyrightability of the Toner Loading Program, which SCC's microchip copied. It determined that Lexmark was unlikely to prevail on its infringement claim because the very short TLP was primarily functional, rather than expressive; because any expression in the choice among alternatives to perform its function was *de minimis*; and because the TLP served as a lock-out code, so copying was necessary for compatibility. Moreover, SCC's use would likely be deemed a fair, transformative use.]

Enacted in 1998, the DMCA has three liability provisions. The statute first prohibits the circumvention of "a technological measure that effectively controls access to a work

protected [by copyright]." 17 U.S.C. § 1201(a)(1). The statute then prohibits selling devices that circumvent access-control measures:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that-
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a [copyrighted work];
>
> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a [copyrighted work]; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a [copyrighted work].

Id. § 1201(a)(2). The statute finally bans devices that circumvent "technological measures" protecting "aright" of the copyright owner. *Id.* § 1201(b). The last provision prohibits devices aimed at circumventing technological measures that allow some forms of "access" but restrict other uses of the copyrighted work,*see Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 441 (2d Cir. 2001); *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1120 (N.D. Cal. 2002), such as streaming media, which permits users to view or watch a copyrighted work but prevents them from downloading a permanent copy of the work, *see RealNetworks, Inc. v. Streambox, Inc.*, 2000 U.S. Dist. LEXIS 1889, No. 2:99CV02070, 2000 WL 127311, at *1-2 (W.D. Wash. Jan. 18, 2000).

The statute also contains three "reverse engineering" defenses. A person may circumvent an access control measure "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 [that person]." 17 U.S.C. § 1201(f)(1). A person "may develop and employ technological means" that are "necessary" to enable interoperability. *Id.* § 1201(f)(2). And these technological means may be made available to others "solely for the purpose of enabling interoperability of an independently created computer program with other programs."*Id.* § 1201(f)(3). All three defenses apply only when traditional copyright infringement does not occur and only when the challenged actions (in the case of the third provision) would not violate other "applicable laws."*Id.*

In filing its complaint and in its motion for a preliminary injunction, Lexmark invoked the second liability provision -- the ban on distributing devices that circumvent access-control measures placed on copyrighted works. *See id.* § 1201(a)(2). According to Lexmark, SCC's SMARTEK chip is a "device" marketed and sold by SCC that "circumvents" Lexmark's "technological measure" (the SHA-1 authentication sequence,

not the checksum operation), which "effectively controls access" to its copyrighted works (the Toner Loading Program and Printer Engine Program). Lexmark claims that the SMARTEK chip meets all three tests for liability under § 1201(a)(2): (1) the chip "is primarily designed or produced for the purpose of circumventing" Lexmark's authentication sequence, 17 U.S.C. § 1201(a)(2)(A); (2) the chip "has only limited commercially significant purpose or use other than to circumvent" the authentication sequence,*id.* § 1201(a)(2)(B); and (3) SCC "markets" the chip "for use in circumventing" the authentication sequence, *id.* § 1201(a)(2)(C). The district court agreed and concluded that Lexmark had shown a likelihood of success under all three provisions.

We initially consider Lexmark's DMCA claim concerning the Printer Engine Program, which (the parties agree) is protected by the general copyright statute. In deciding that Lexmark's authentication sequence "effectively controls access to a work protected under [the copyright provisions]," the district court relied on a definition in the DMCA saying that a measure "effectively controls access to a work" if, "in the ordinary course of operation," it "requires the application of information, or a process or treatment, with the authority of the copyright owner, to gain access to the work." 17 U.S.C. § 1201(a)(3). Because Congress did not explain what it means to "gain access to the work," the district court relied on the "ordinary, customary meaning" of "access": "the ability to enter, to obtain, or to make use of," D. Ct. Op. at 41 (quoting *Merriam-Webster's Collegiate Dictionary* 6 (10th ed. 1999)). Based on this definition, the court concluded that "Lexmark's authentication sequence effectively 'controls access' to the Printer EngineProgram because it controls the consumer's ability to *make use of* these programs." D. Ct. Op. at 41 (emphasis added).

We disagree. It is not Lexmark's authentication sequence that "controls access" to the Printer Engine Program. *See* 17 U.S.C. § 1201(a)(2). It is the purchase of a Lexmark printer that allows "access" to the program. Anyone who buys a Lexmark printer may read the literal code of the Printer Engine Program directly from the printer memory, with or without the benefit of the authentication sequence, and the data from the program may be translated into readable source code after which copies may be freely distributed. No security device, in other words, protects access to the Printer Engine Program Code and no security device accordingly must be circumvented to obtain access to that program code.

The authentication sequence, it is true, may well block one form of "access" -- the "ability to . . . make use of" the Printer Engine Program by preventing the printer from functioning. But it does not block another relevant form of "access" -- the "ability to [] obtain" a copy of the work or to "make use of" the literal elements of the program (its code). Because the statute refers to "controlling access to a work protected under this title," it does not naturally apply when the "work protected under this title" is otherwise accessible. Just as one would not say that a lock on the back door of a house "controls access" to a house whose front door does not contain a lock and just as one would not say that a lock on any door of a house "controls access" to the house after its purchaser receives the key to the lock, it does not make sense to saythat this provision of the DMCA applies to otherwise-readily-accessible copyrighted works. Add to this the fact

that the DMCA not only requires the technological measure to "control[] access" but also requires the measure to control that access "effectively," 17 U.S.C. § 1201(a)(2), and it seems clear that this provision does not naturally extend to a technological measure that restricts one form of access but leaves another route wide open. *See also id.* § 1201(a)(3) (technological measure must "*require*[] the application of information, or a process or a treatment . . . to gain access to the work") (emphasis added). *See Chamberlain Group, Inc. v. Skylink Techs., Inc..*, 381 F.3d 1178, 1198, 2004 U.S. App. LEXIS 18513, at *52 (Fed. Cir. Aug. 31,2004)* ("Chamberlain's proposed construction of the DMCA ignores the significant differences between defendants whose accused products enable copying and those, like Skylink, whose accused products enable only legitimate uses of copyrighted software.").

Nor are we aware of any cases that have applied this provision of the DMCA to a situation where the access-control measure left the literal code or text of the computer program or data freely readable. And several cases apply the provision in what seems to us its most natural sense. *See, e.g.*, *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1095 (N.D. Cal. 2004) (deciding that the "CSS" encryption program, which prevents viewing of DVD movies and copying of the data encoded on the DVD, effectively controls access to copyrighted DVD movies); *Universal City Studios, Inc. v. Reimerdes*,111 F. Supp. 2d 294, 318 (S.D.N.Y. 2000), *aff'd sub nom.*, *Corley*, 273 F.3d 429; *Sony Computer Entm't Am. Inc. v. Gamemasters*, 87 F. Supp. 2d 976, 987 (N.D. Cal. 1999) (deciding that technological measure on PlayStation game console, which prevented unauthorized games from being played, effectively controlled access to copyrighted CD-ROM video games, which the facts of the case do not describe as either encrypted or unencrypted); *see also* *RealNetworks,* 2000 U.S. Dist. LEXIS 1889, 2000 WL 127311, at *3 (noting that the technological measure at issue was a "successful means of protecting against unauthorized duplication and distribution" of copyrighted digital works); *Pearl Invs. LLC v. Std. I/O, Inc.*, 257 F. Supp. 2d 326, 349-50 (D.Me. 2003) (determining that plaintiff's "encrypted, password-protected virtual private network," which blocked access to data including plaintiff's copyrighted computer software, was a technological measure that effectively controlled access to that work).

…Lexmark counters that several cases have embraced a "to make use of" definition of "access" in applying the DMCA. While Lexmark is partially correct, these cases (and others as well) ultimately illustrate the liability line that the statute draws and in the end explain why access to the PrinterEngine Program is not covered.

In the essential setting where the DMCA applies, the copyright protection operates on two planes: in the literal code governing the work and in the visual or audio manifestation generated by the code's execution. For example, the encoded data on CDs translates into music and on DVDs into motion pictures, while the program commands in software for video games or computers translate into some other visual and audio manifestation. In the cases upon which Lexmark relies, restricting "use" of the work means restricting consumers from making use of the copyrightable expression in the work. *See 321 Studios*, 307 F. Supp. 2d at 1095 (movies contained on DVDs protected by an encryption algorithm cannot be watched without a player that contains an access key); *Reimerdes,*

111 F. Supp. 2d at 303 (same); *Gamemasters, 87 F. Supp. 2d at 981* (Sony's game console prevented operation of unauthorized video games). As shown above, the DMCA applies in these settings when the product manufacturer prevents all access to the copyrightable material and the alleged infringer responds by marketing a device that circumvents the technological measure designed to guard access to the copyrightable material.

The copyrightable expression in the Printer Engine Program, by contrast, operates on only one plane: in the literal elements of the program, its source and object code. Unlike the code underlying video games or DVDs, "using" or executing the Printer Engine Program does not in turn create any protected expression. Instead, the program's output is purely functional: the Printer Engine Program "controls a number of operations" in the Lexmark printer such as "paper feed[,] paper movement[,] [and] motor control." Lexmark Br. at 9; *cf. Lotus Dev., 49 F.3d at 815* (determining that menu command hierarchy is an "uncopyrightable method of operation"). And unlike the code underlying video games or DVDs, no encryption or other technological measure prevents access to the Printer Engine Program. Presumably, it is precisely because the Printer Engine Program is not a conduit to protectable expression that explains why Lexmark (or any other printer company) would not block access to the computer software that makes the printer work. Because Lexmark's authentication sequence does not restrict access to this literal code, the DMCA does not apply.

Lexmark next argues that access-control measures may "effectively control access" to a copyrightedwork within the meaning of the DMCA even though the measure may be evaded by an "'enterprising end-user.'" Lexmark Br. at 46 (quoting *RealNetworks, 2000 U.S. Dist. LEXIS 1889, 2000 WL 127311, at *9*). Doubtless, Lexmark is correct that a precondition for DMCA liability is not the creation of an impervious shield to the copyrighted work.*See RealNetworks, 2000 U.S. Dist. LEXIS 1889, 2000 WL 127311, at *9*; *Reimerdes, 111 F. Supp. 2d at 317-18* (rejecting argument that an encryption measure does not "effectively control access" because it is only a "weak cipher"); *see also* 17 U.S.C. § 1201(a)(3). Otherwise, the DMCA would apply only when it is not needed.

But our reasoning does not turn on the *degree* to which a measure controls access to a work. It turns on the textual requirement that the challenged circumvention device must indeed circumvent *something*, which did not happen with the Printer Engine Program. Because Lexmark has not directed any of its security efforts, through its authentication sequence or otherwise, to ensuring that its copyrighted work (the Printer Engine Program) cannot be read and copied, it cannot lay claim to having put in place a "technological measure that effectively controls access to a work protected under [the copyright statute]."17 U.S.C. § 1201(a)(2)(B).

Nor can Lexmark tenably claim that this reading of the statute fails to respect Congress's purpose in enacting it. Congress enacted the DMCA to implement the Copyright Treaty of the World Intellectual Property Organization, and in doing so expressed concerns about the threat of "massive piracy" of digital works due to "the ease with which [they] can be copied and distributed worldwide virtually instantaneously." S. Rep. No. 105-190,

at 8 (1998). As Congress saw it, "copyrighted works will most likely be encrypted and made available to consumers once payment is made for access to a copy of the work.[People] will try to profit from the works of others by decoding the encrypted codes protecting copyrighted works, or engaging in the busine ss of providing devices or services to enable others to do so." H.R. Rep. No. 105-551, pt. 1, at 10. Backing with legal sanctions "the efforts of copyright owners to protect their works from piracy behind digital walls such as encryption codes or password protections," *Corley*, 273 F.3d at 435, Congress noted, would encourage copyright owners to make digital works more readily available, *see* S. Rep. No. 105-190, at 8. *See also* Nimmer § 12A.02[B][1].

Nowhere in its deliberations over the DMCA did Congress express an interest in creating liability for the circumvention of technological measures designed to prevent consumers from using consumer goods while leaving the copyrightable content of a work unprotected. In fact, Congress added the interoperability provision in part to ensure that the DMCA would not diminish the benefit to consumers of interoperable devices "in the consumer electronics environment." 144 Cong. Rec. E2136 (daily ed. Oct. 13, 1998)(remarks of Rep. Bliley). *See generally* Anti-Circumvention Rulemaking Hearing, at 44-56, at http://www.copyright.gov/1201/2003/hearings/transcript- may9.pdf (testimony of Professor Jane Ginsburg) (Section 1201(a) does not "cover[] the circumvention of a technological measure that controls access to a work not protected under [the Copyright] title. And if we're talking about ball point pen cartridges, printer cartridges, garage doors and so forth, we're talking about works not protected under this title.").

In view of our conclusion regarding the Printer Engine Program, we can dispose quickly of Lexmark's DMCA claim regarding the Toner Loading Program. The SCC chip does not provide "access" to the Toner Loading Program but replaces the program. And to the extent a copy of the Toner Loading Program appears on the Printer Engine Program, Lexmark fails to overcome the same problem that undermines its DMCA claim with respect to the Printer Engine Program: Namely, it is not the SCC chip that permits access to the Printer Engine Program but the consumer's purchase of the printer. One other point deserves mention. All three liability provisions of this section of the DMCA require the claimant to show that the "technological measure" at issue "controls access to *a work protected under this title*," *see* 17 U.S.C. § 1201(a)(2)(A)-(C), which is to say a work protected under the general copyright statute, *id.* § 102(a). To the extent the Toner Loading Program is not a "work protected under [the copyright statute],"which the district court will consider on remand, the DMCA necessarily would not protect it.

The district court also rejected SCC's interoperability defense -- that its replication of the Toner Loading Program data is a "technological means" that SCC may make "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). In rejecting this defense, the district court said that "SCC's SMARTEK microchips cannot be considered independently created computer programs. [They] serve no legitimate purpose other than to circumvent Lexmark's authentication sequence and . . . cannot qualify as independently created when they contain exact copies of Lexmark's Toner Loading Programs." D. Ct.

Op. P 94, at 47.

Because the issue could become relevant at the permanent injunction stage of this dispute, we briefly explain our disagreement with this conclusion. In particular, the court did not explain why it rejected SCC's testimony that the SMARTEK chips do contain other functional computer programs beyond the copied Toner Loading Program data. The affidavit of Lynn Burchette, an SCC manager, states that "[the SMARTEK] chip has a microprocessor, with software routines we developed that control its operation and function. Our chip supports additional functionality performed by our software beyond that of [the chip on Lexmark's toner cartridges]." JA 103. And Dr. Goldberg testified that "Static Control has written a substantial amount of software for managing this chip; for not only providing the interoperability features, but also for managing the additional functionality that the [chip manufacturer] provides and which the remanufacturers may want." … SCC also has satisfied the "independently created computer programs" requirement and may benefit from the interoperability defense, at least in the preliminary injunction context. …

Because Lexmark failed to establish a likelihood of success on any of its claims, whether under the general copyright statute or under the DMCA, we vacate the district court's preliminary injunction and remand the case for further proceedings consistent with this opinion.

CONCURRENCE: MERRITT, J.

…I write separately to emphasize that our holding should not be limited to the narrow facts surrounding either the Toner Loading Program or the Printer Engine Program. We should make clear that in the future companies like Lexmark cannot use the DMCA in conjunction with copyright law to create monopolies of manufactured goods for themselves just by tweaking the facts of this case: by, for example, creating a Toner Loading Program that is more complex and "creative" than the one here, or by cutting off other access to the Printer Engine Program. The crucial point is that the DMCA forbids anyone from trafficking in any technology that "is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a [protected] work." 17 U.S.C. § 1201(a)(2)(A) (emphasis added). The key question is the "purpose" of the circumvention technology. The microchip in SCC's toner cartridges is intended not to reap any benefit from the Toner Loading Program - SCC's microchip is not designed to measure toner levels - but only for the purpose of making SCC's competing toner cartridges work with printers manufactured by Lexmark.

…For these additional reasons, I concur in the Court's opinion reversing the judgment of the district court. On remand the first question should be whether Lexmark can show the requisite "primary purpose" to pirate a copyrighted work rather than to ensure that their own cartridges work with Lexmark's printer. If not, its case against SCC should be dismissed.

The Broadcast Flag: It's not just TV
57 Fed. Comm. L.J. 209 (2005)
Wendy Seltzer[1]

I'm not much of a television person. My only set, non-HD, still picks up its channels through rabbit ears. The broadcast flag still gets me steamed, though, so much so that I recently built a high-definition digital video recorder just to beat the flag mandate.

It's not about the television. Or rather, it's not about television as broadcast to the passive consumer, to be received on single-purpose boxes. It's about television as it could be, with innovative companies and tinkerers making television broadcasts a core part of the converged home media network. The crippling of this kind of television is an early warning against a pervasive technology regulation.

The broadcast flag represents a bad detour for the Federal Communications Commission, a heavily regulatory regime introduced in a period of supposed deregulation. Because the threats of this technology mandate echo through other regulations, it pays to dig into the details of "Redistribution Controls" and "Covered Demodulators"[2] to understand how quickly "digital broadcast content protection" becomes technology licensing.

Like standard definition analog programming, digital television is broadcast free, unencrypted, over the public airwaves. Equipped with the proper antenna and demodulator, any device can see this signal and convert it to a stream of bits (the ones and zeros of digital content), then translate those bits into the audio and video of television programming. The "broadcast flag" is a single bit's worth of information in that signal: "flagged" or "unflagged." "Flagged" conveys the "do not redistribute" demand.

The Commission proposed and then adopted this scheme at the urging of motion picture studios, who threatened to withhold content from digital television unless they were given copy protection.[3] But a flag on a signal transmitted in the clear can serve at most as advisory notification, like the "please do not forward" footer some people include in email that they send unencrypted.[4] Since mere notification could be bypassed, the Commission further determined to bake flag recognition into "robust" DTV hardware.

---

[1] Wendy Seltzer, wendy@seltzer.com, is an attorney and special projects coordinator at the Electronic Frontier Foundation, an online civil liberties organization that has challenged the broadcast flag as a plaintiff in *American Library Association et al. v. FCC*.
[2] *In the Matter of Digital Broadcast Content Protection*, MB Docket No. 02-230, Report and Order and Further Notice of Proposed Rule, FCC No. 03-273 (rel. Nov. 4, 2003) (hereafter, "Broadcast Flag Order").
[3] *See* Notice of Proposed Rulemaking, FCC No. 02-231 (Aug. 8, 2002).
[4] I thank my colleague Seth David Schoen for the email analogy. Spelled out, it illustrates how easily tech mandates devolve into full-fledged technology regulation: To implement its "do not forward" regulation, the Funny Commands Commission would have to redesign all email software to ensure that every program written watched for and responded to "do not forward" flag. That includes programs running the gamut from Microsoft Outlook, to the Blackberry client, to open-source clients mutt and pine, to the few-line program written in a basic networking class.

The Broadcast Flag Order, issued in late 2003, mandates that every device capable of demodulating or receiving the DTV signal watch for the flag and impose its limitations. These devices must permit the signal to pass only through "approved" outputs (analog, re-modulated, low-resolution digital, or an "approved output content protection technology") and only to "approved digital recording technology." Broadcast Flag Order at 22, ¶ 42. All such devices must be robust against user modifications that might give access to the original digital signal. *Id*., ¶ 46. After July 1, 2005, it is unlawful to manufacture or import a non-compliant demodulator for sale in interstate commerce. *Id*., 47 CFR §73.9002.

Thus the Commission's regulation is not ultimately about communications, but about the devices that receive them:

> We conclude that in order for a flag-based content protection system to be effective, demodulators integrated within, or produced for use in, DTV reception devices ("Demodulator Products") must recognize and give effect to the ATSC flag pursuant to the compliance and robustness rules …. This necessarily includes PC and IT products that are used for off-air DTV reception.

Broadcast Flag Order at 21, ¶ 40.

The Broadcast Flag Order aims at a copyright problem, studios' fear of "indiscriminate redistribution" of their copyrighted content, but it isn't typical copyright law. Instead of focusing on infringing uses of TV broadcasts (taping a show and selling copies, for example), this new kind of regulation puts the government in the business of redesigning products that *might* be used to infringe. In the process, it locks out many non-infringing uses, innovative technologies, competitive products, and open-source developers. Because these collateral harms are unavoidable, technology mandates should be a last resort, not a predictive strike against hypothetical danger.

The HD-PVR I built – a general-purpose PC, an HD tuner card, and the free and open-source GNU/Linux operating system and MythTV software[5] – beats anything on the commercial market for flexibility and programmability. With it, I can record over-the-air HD broadcasts, watch them live, time-shifted, or at double speed; remotely program the PVR to capture a show a friend recommends; play recordings back on a frontend anywhere else on the network; or excerpt clips from recorded shows. I can do this from the same place I manage my music, home movie, and photo collections.

After the flag mandate takes effect, however, it will be impossible to build this machine with new parts. The HD tuner inside has open interfaces, giving access to the full digital signal for recording and replaying. It's not "robust" against user modification, a requirement by definition incompatible with open source. It's not that anything I do with the tuner card or HD-PVR infringes copyright, but the fact that the card offers

---

[5] *See* the full setup at <http://www.eff.org/broadcastflag/cookbook/>. MythTV, initially programmed by Isaac Richards , now has more than 20 active developers and hundreds of users.

"uncontrolled" outputs and fails to watch for the broadcast flag that will make it and others like it unlawful to manufacture.

The Broadcast Flag rule means I can't tinker with my TV. It means others can't either, including the technologists who might want to bring us the next great advance like TiVo. They have to engineer to government approval, more than consumer demand or technological requirements. Before they could bring a new product near market, they'd have to hire a bevy of lawyers to seek Commission approval or to obtain a license for an existing approved technology, with complex licensing requirements and restrictions that often surpass those of the Commission's mandate.[6] By the time the technology escaped that process, if it emerged at all, it would likely have had the life sucked out of it in the name of "compliance."

The DTV devices on the market this July will lack high-resolution, clear, digital outputs that can feed seamlessly into other devices. To ensure that the "do-not-redistribute" bit stays firmly affixed to its signal, devices will restrict users' ability to export the content, and use encryption and dongles to ensure that they communicate only with their own, restrictive, kind. Watching DTV is, as Susan Crawford puts it, "like being bitten in the neck by a vampire": Once one piece of the home media network has been bitten by DTV, all others must be infected by the same standard.[7]

Even among restricted devices, there will be incompatibilities: You can't just pull a tape (or DVD) from one machine and put it in another. The TiVo HD-video recorder might not be able to communicate with Sony MagicGate hardware or a RealNetworks Helix-enabled device. For unless they're designed together, devices might not know whether their downstream neighbors would respect the flag limitations or leak. And just when you have the home network running smoothly, any of the DTV devices can have its HD privileges "revoked" at any time.

Thus the Broadcast Flag's technology mandate vitiates copyright's fair use doctrine – the principle that some uses of copyrighted material are permissible without authorization of the copyright holders. If some fair uses are technically blocked by all devices lawfully made for sale, those uses are as good as gone.

Although the Supreme Court has said, "[t]he task [of fair use analysis] is not to be simplified with bright-line rules, for the statute, like the doctrine it recognizes, calls for case-by-case analysis," (*Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 577 (1994)) technology cannot pull in a judge to analyze each case. Any technological implementation of fair use must therefore be a rough cut, and the cuts the broadcast flag gives us are particularly rough. Recording a show to watch on another device might be fair, to watch it later, or unfair, to duplicate and sell; excerpting clips from the evening news for redistribution might be fair, to create your own parodic "Daily Show," or unfair, to make a competing cut-rate newscast, but the technologies approved under the

---

[6] See, e.g., licensing requirements for HDCP, DTCP, or Windows Media DRM, MB Dockets No. 04-61, 04-64, and 04-66, described in Order approving 13 technologies, FCC 04-193, August 12, 2004.

[7] Zeller, *Federal Effort to Head Off TV Piracy Is Challenged*, New York Times, Feb. 21, 2005, online at <http://www.nytimes.com/2005/02/21/technology/21flag.html?ex=1109653200&en=f831bf942e767caf&ei=5070>

Commission's initial certification, and the devices implementing them, presume unfair what they can't control.

The technical specifications of the broadcast flag mandate do not explicitly foreclose fair use copying. Indeed, the Commission repeatedly states that "our goal of preventing the indiscriminate redistribution of digital broadcast television content 'will not (1) interfere with or preclude consumers from copying broadcast programming and using or redistributing it within the home or similar personal environment as consistent with copyright law.'"[8] But much fair use copying or interoperability falls into the gap between the rule and its implementation.

Twenty years ago, while Universal Studios was suing Sony Electronics for producing the Betamax video tape recorder, Universal suggested that Sony should have engineered its devices to respond to a broadcast flag marking programs unauthorized for recording. The Supreme Court majority, ruling in Sony's favor, rejected that suggestion and held that "time-shifting" broadcast television was fair use, even without the authorization of the copyright holder. *Sony Corp. v. Universal City Studios*, 464 U.S. 417 (1984) The Court had never addressed this kind of fair use before; anyone trying to encode *existing* "legitimate uses" of broadcast television might well have coded it out of the picture. Yet the fair and previously unanticipated use prevailed. The *Sony* Court refused content owners' request to hold the public's rights and abilities static in the face of new technologies. Fast-forward twenty years, however, and that is precisely what the Commission has done in this rulemaking. The Broadcast Flag Order precludes the next fair use that has not yet been invented.

Under the Broadcast Flag regime, market participants, bound up in the welter of licensing and pre-approval requirements can't offer the products users want. Where the market fails to provide fair-use-enabling technologies, the robustness rules prevent end-users from correcting the problem. Absent technology mandates, users dissatisfied with commercial options can and do write their own software alternatives (and often share them in open-source). In a world of restricted, robust hardware, users are limited to the options the commercial market provides: the fully-capable hardware HD tuner card can't be manufactured. Consumer-driven innovation is cut off when users can't tinker with existing technologies or develop new ones that challenge market leaders.

Finally, the broadcast flag, like other roadblocks designed to "keep honest people honest" is both over- and under-inclusive. It stops the "honest people" from legitimate non-infringing activities, while it doesn't stop the dedicated pirates, who will still have legacy devices, the analog hole, and the ability to hire experts to build their own demodulators.[9] Honest people don't need technologically enforced barriers, while dishonest people aren't deterred by them.

---

[8] Order approving 13 technologies, FCC 04-193, August 12, 2004 (quoting Broadcast Flag Order, 18 FCC Rcd. at 23555).

[9] For the idea that it takes only one leak to seed unauthorized distribution of high-value content, *see* Biddle, England, Peinado, and Willman, "The Darknet and the Future of Content Distribution," presented at the 2002 ACM Workshop on Digital Rights Management, November 18, 2002 (available at <http://crypto.stanford.edu/DRM2002/darknet5.doc>).

Limits on open source development, on interoperability, on technological innovation, and on fair use, are not merely incidental to this implementation of a Broadcast Flag technology mandate. The burdens, and the Broadcast Flag's over- and under-inclusiveness in addressing the concerns that motivated it, are inherent in a technology mandate. At the intersection of multiple regulatory modes – law, code, and markets[10] – public rights are hard-coded out.

Copyright holders have long desired the kind of control technology mandates offer. If they get to oppose new technologies before they come to market, before they disrupt existing distribution models, the studios can keep doing business as they have and blame any downturns on "piracy." After motion picture studios' apparent success with the digital television Broadcast Flag, members of the recording industry have gone to the Commission asking for their own broadcast flag for digital radio.[11]

Nor is the regulatory urge of tech mandates limited to copyright holders. In August 2004, the Commission opened a Noticed of Proposed Rulemaking in response to a joint petition of the Department of Justice, the Federal Bureau of Investigation, and the Drug Enforcement Administration requesting expansion of the Communications Assistance for Law Enforcement Act (CALEA) to cover communications that travel over the Internet. If the Commission were to accede to their demands as well, broadband providers would be required to rebuild their networks to make it easier for law enforcement to tap Internet "phone calls" that use Voice over Internet Protocol, or online "conversations" using various instant messaging programs such as AOL Instant Messenger or Jabber. Once again, open source implementations of these protocols might be precluded because they couldn't keep the tappability mandate built-in.

The Commission should recognize the extreme regulation all of these tech mandates require and reject intrusive regulation here as it has elsewhere.

---

[10] *See* Lawrence Lessig, *Code and other Laws of Cyberspace* (Basic Books, 1999).
[11] *See* FCC MM Docket No. 99-325.