

NELCO
NELCO Legal Scholarship Repository

Columbia Public Law & Legal Theory Working
Papers

Columbia Law School

8-1-2005

Legal Protection of Technological Measures Protecting Works of Authorship: International Obligations and the US Experience

Jane C. Ginsburg
Columbia Law School, ginsburg@law.columbia.edu

Follow this and additional works at: http://lsr.nellco.org/columbia_pllt

 Part of the [Intellectual Property Commons](#), and the [Public Law and Legal Theory Commons](#)

Recommended Citation

Ginsburg, Jane C., "Legal Protection of Technological Measures Protecting Works of Authorship: International Obligations and the US Experience" (2005). *Columbia Public Law & Legal Theory Working Papers*. Paper 0593.
http://lsr.nellco.org/columbia_pllt/0593

This Article is brought to you for free and open access by the Columbia Law School at NELCO Legal Scholarship Repository. It has been accepted for inclusion in Columbia Public Law & Legal Theory Working Papers by an authorized administrator of NELCO Legal Scholarship Repository. For more information, please contact tracy.thompson@nellco.org.

Legal Protection of Technological Measures Protecting Works of Authorship: International Obligations and the US Experience

Jane C. Ginsburg*

Abstract

The ongoing transposition of the EU Information Society Directive's requirement that member States adopt of legal prohibitions of the circumvention of technological protections of works of authorship occasions this review of international obligations and their implementation in the US. This article addresses the scope of international obligations the WIPO Copyright Treaties impose on member States to protect against circumvention, as well as the US experience with the Digital Millennium Copyright Act's prohibitions on circumvention of access and copy controls. It examines the text of the statute, codified at sec. 1201 of the 1976 Copyright Act, the five years of judicial decisions interpreting the statute, and the two administrative proceedings implementing one aspect of the statutory scheme. The analysis of the DMCA and its judicial and administrative interpretation will take up three issues:

- 1) What technological measures does sec. 1201 protect?
- 2) What conduct does sec. 1201 prohibit?
- 3) To what extent does sec. 1201 accommodate copyright exceptions?

The US experience to date indicates that legal protection for technological measures has helped foster new business models that make works available to the public at a variety of price points and enjoyment options, without engendering the "digital lockup" and other copyright owner abuses that many had feared. This is not to say that the US legislation and its judicial interpretation represent the most preferable means to making the internet a hospitable place for authors while continuing to enable lawful user conduct. But brooding forecasts and legitimate continuing concerns notwithstanding, the overall equilibrium so far appears to be a reasonable one.

Introduction

The ongoing (belated) transposition of the EU Information Society Directive's requirement that member States adopt of legal prohibitions of the circumvention of technological protections of works of authorship¹ has made this topic both current and contentious. This article wades into that rhetorically-charged fray in two different, but, I hope, analytically rigorous, ways. First, following some general observations concerning the impetus for copyright holder resort to technological protection measures, I will consider the scope of international obligations the WIPO Copyright Treaties impose on member States to protect against circumvention. Second, I will address the US experience with the Digital Millennium Copyright Act's prohibitions on circumvention of

* Morton L Janklow Professor of Literary and Artistic Property Law, Columbia University School of Law; visiting Goodhart Chair of Legal Science, University of Cambridge. This article is based on a lecture given at the University of Oslo Faculty of Law, May 18, 2005.

¹ Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *Official Journal L 167*, 22/06/2001 P. 0010 - 0019. Article 6 addresses technological protection measures; article 13(1) required member States to have implemented the Directive's norms by Dec 22, 2002.

access and copy controls. I will consider the text of the statute, codified at sec. 1201 of the 1976 Copyright Act, the five years of judicial decisions interpreting the statute, and the two administrative proceedings implementing one aspect of the statutory scheme. The analysis of the DMCA and its judicial and administrative interpretation will take up three issues:

- 1) What technological measures does sec. 1201 protect?
- 2) What conduct does sec. 1201 prohibit?
- 3) To what extent does sec. 1201 accommodate copyright exceptions?

By examining one national system where legal protections for technological measures have been in place for some time, I hope to contribute modestly toward the discussions in Europe concerning the implementation of the EU and WIPO Treaties' directive to provide adequate legal protection against the circumvention of effective technological measures.² The US experience to date indicates that legal protection for technological measures has helped foster new business models that make works available to the public at a variety of price points and enjoyment options, without engendering the "digital lockup" and other copyright owner abuses that many had feared.³ This is not to say that the US legislation and its judicial interpretation have found the magic formula for making the internet a hospitable place for authors while continuing to enable lawful user conduct. But brooding forecasts and legitimate continuing concerns notwithstanding, the overall equilibrium so far appears to be a reasonable one.

Let me turn to the general policy question: Why establish an international obligation requiring legal protection for technological protections of copyrighted works? As many commentators and other authorities have recognized, in the digital environment, the ease of copying may render legal protection *simpliciter* inadequate.⁴ In the past, copying technology was too rudimentary, cumbersome or expensive to enable users to

² See WIPO Copyright Treaty art. 11; WIPO Performers and Phonograms Treaty art. 18; Information Society Directive, *supra*, art. 6.

³ On fear and loathing of legal protection for technological measures, see, e.g., Jonathan Band & Taro Ishiki, *The New Anti-Circumvention Provision in the Copyright Act: A Flawed First Step*, CYBERSPACE LAW, Feb. 1999, at 2; Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 BERKELEY TECH. L.J. 519 (1999); Jessica Litman, *The Breadth of the Anti-Trafficking Provisions and the Moral High Ground*, in ADJUNCTS AND ALTERNATIVES TO COPYRIGHT: PROCEEDINGS OF THE ALAI CONGRESS JUNE 13-17, 2001 456 (Jane C. Ginsburg & June M. Besek eds., 2002); Kamiel Koelman, *The Protection of Technological Measures vs. the Copyright Limitations*, in ADJUNCTS AND ALTERNATIVES at 448; Thomas C. Vinje, *A Brave New World of Technical Protection Systems: Will There Still Be Room for Copyright?*, 18 EUR. INTELL. PROP. REV. 431 (1996).

⁴ See, e.g., US Working Group on Intellectual Property Rights of the Task Force on the National Information Infrastructure WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS, INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 230 (1995); Jörg Reinbothe and Silke von Lewinski, *The WIPO Treaties 1996* 135-37 (2002); Mihály Ficsor, *The Law of Copyright and the Internet: The 1996 WIPO Treaties, Their Interpretation and Implementation*, 359-406 (2002); Séverine Dusollier, *Droit d'auteur et protection des oeuvres dans l'univers numérique - Droits et exceptions à la lumière des dispositifs de verrouillage des oeuvres* [page cite] (2005).

copy and disseminate on the scale that digital media make possible.⁵ Copyright law's prohibitions thus generally sufficed, because right holders could enforce the law against the commercial intermediaries who engaged in large scale copying and dissemination, while whatever copying end users engaged in was unlikely to rival the copyright owner's control of markets for the work. When digital media changed the technological balance, they also altered legal relationships, for now economically significant infringing acts were no longer the sole province of entities higher up the distribution chain. To redress the shift, it might be necessary to reinforce the legal prohibition with a layer of technological protection, disabling end users from availing themselves of some of the copying technology's potential for reproducing and redistributing copyrighted works.

But supplying a technological lock may offer only short-lived solace: the measure may be effective only for so long as it takes to develop and distribute a device to break it. If end users may easily procure the means to circumvent technological impediments, then we are back where we started, without a middleman against whom copyright may effectively be enforced. Hence the conclusion followed that legal protection supplemented by technological protection will fail unless the technological protection is in turn backed up by further legal protection against the provision of circumvention devices or services.⁶ When the copyists are so diffuse, the intermediary whom the enforcement efforts target now becomes the distributor of the means to circumvent technological protections.

The mandates of the 1996 WIPO Copyright Treaties stem from this recognition. Moreover, the drafters of the WCT and WPPT were not writing on an entirely clean slate, for WIPO had itself previously considered proposing dispositions prohibiting the distribution of "unauthorized decoders" of encrypted television transmissions.⁷ In addition, the European Commission had in 1991 already required member States to prohibit "any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a

⁵See, e.g., I. Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U. Chi. Legal F. 217, 224-25 (discussing "state of the art" limitations on unauthorized copying and exploitation).

⁶For an evocation and analysis of this three-layer approach, see, e.g., Alain Strowel., *La protection des mesures techniques: une couche en trop?*, Auteurs & Médias, 2001, p. 90-95. Séverine Dusollier, *Droit d'auteur et protection des oeuvres dans l'univers numérique - Droits et exceptions à la lumière des dispositifs de verrouillage des oeuvres* (2005). As Professor Sirinelli has observed, "Technology comes to the aid of rights threatened by technology. But can it do everything? In order to be really effective, the devices themselves have to be protected. The WIPO Treaties . . . provide such measures. In a never-ending game of mirrors, rights come to the aid of technology so as to allow the latter to come to the aid of rights . . .!!!" Pierre Sirinelli, *Exceptions and limitations to copyright and neighboring rights*, Report presented to the Workshop on Implementation Issues of the WIPO Copyright Treaty (WCT) and the WIPO Performers and Phonograms (WPPT), Geneva, December 6-7, 1999, WIPO Doc. WCT-WPPT/IMP/1 p. 28 (Dec. 3, 1999).

⁷See Committee of Experts on Model Provisions in the Field of Copyright, Third Session (Geneva, July 2-13, 1990) Copyright September 1990, Preparatory Document, at para. 319-38. The Committee of Experts also considered requiring the provision of equipment that would limit the ability of home recording machines to make successive generations of digital copies, see id., para. 303-17. The proposal would have included an early form of copyright management information, see para. 312.

computer program.”⁸ Similarly, in 1992, the US Audio Home Recording Act required all “digital audio recording devices” to be equipped with the “serial copying management system,” which disabled multigenerational copying of digital musical recordings. The Act also prohibited the distribution of any device or provision of any service “the primary purpose or effect of which is to . . . circumvent” the system.⁹ More generally, many national laws contained a variety of provisions in their tort or unfair competition laws, as well as in their telecommunication and penal laws, prohibiting a range of circumvention-related conduct such as the sale of satellite descramblers, and computer hacking.¹⁰

I. Subject matter and scope of the international obligation

Article 11 of the WCT provides:

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

We will consider the subject matter as well as the scope of protection that the WCT requires member States to provide.¹¹

Subject matter protected – “effective technological measures”: The WCT does not define what makes a technological protection measure “effective.” The term, which recurs in national and regional laws implementing art. 11,¹² is not self-explanatory.¹³ The one thing it cannot mean is “impervious.” That is, were the measure not “effective” unless it resisted attempts to circumvent it, there would be no need for legal protection; the technology would take care of itself. If “effective” simply means that it hinders or prevents the relevant copyright-implicating act¹⁴ -- copying, distributing, communicating

⁸ COUNCIL DIRECTIVE of 14 May 1991 on the legal protection of computer programs (91/250/EEC) Official Journal L 122, 17/05/1991 P. 0042 - 0046, art. 7(1)(c).

⁹ 17 U.S.C. § 1002(c).

¹⁰ For a detailed discussion, see Séverine Dusollier, General Report, *Situating Legal Protections for Copyright-Related Technological Measures in the Broader Legal Landscape: Anti Circumvention Protection outside Copyright*, in *Adjuncts and Alternatives to Copyright*, Proceedings of the 2001 ALAI Congress, 123 (Jane Ginsburg and June Besek, eds. 2002) [hereafter *Adjuncts and Alternatives*]. See also the questionnaire related to the General Report, id. at 110.

¹¹ The following analysis of WCT art 11 is adapted from SAM RICKETSON AND JANE C. GINSBURG, *INTERNATIONAL COPYRIGHT AND NEIGHBORING RIGHTS: THE BERNE CONVENTION AND BEYOND* paras. 15.10-15.22 (*forthcoming*, Oxford U. Press 2006).

¹² See, e.g., 17 U.S.C. sec. 1201(a)(1)(A), 1201(b)(1)(A); Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *Official Journal L 167*, 22/06/2001, art. 6

¹³ For a variety of interpretations, see Jacques de Werra, *The Legal System of Technological Protection Measures under the WIPO Treaties, the Digital Millennium Copyright Act, the European Union Directives, and other National Laws*, (Japan, Australia), in *Adjuncts and Alternatives* 198, 207.

¹⁴ See, e.g., 17 U.S.C. sec. 1201(b)(2)(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).

to the public – then it is not clear what the term adds.¹⁵ By contrast, the approach taken in the European Union defines the term to describe the universe of protected measures: in the EU, an “effective” technological measure is one “where the use of a protected work or other subject-matter is controlled by the rightholders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective.”¹⁶ This definition resolves the question of coverage of types of technological measures. It implies, however, that a technological measure that controls neither access nor copying, would not be “effective” (no matter how well it functioned), and therefore would not be protected against circumvention.¹⁷

“Used by authors . . .” In this context, the term “authors” comprehends authors’ successors in title (see Berne. Conv. art. 2(6)). While authors themselves may increasingly apply technological protection measures that enable them to market their works directly to the public without resort to intermediaries who require them to transfer all or part of their copyrights,¹⁸ the WCT text should not be read to limit the protection of technological measures only to those actually applied by authors. Such a reading would disqualify protection of devices used by intermediaries on behalf of authors, thus defeating the WCT’s author-protective goals. Moreover, the difficulty of knowing whether a particular protection measure has been used by the author or by her successor in title would make such an interpretation unworkable.

“. . . in connection with the exercise of their rights under this Treaty or the Berne Convention”: This phrase concerns the types of technological protection measures covered. A measure that prevents or hinders any of the acts covered within Berne or WCT economic or moral rights with respect to protected works would come within art. 11’s scope. Thus, measures protecting against copying (Berne Conv. art. 9), adapting

¹⁵ Reinbothe and von Lewinski, *supra* at 145, suggest that malfunctioning technological measures need not be protected against circumvention, nor should those which “interfere with the normal functioning of the equipment or services,” giving the example of a copy control mechanism that interferes with the playability of a television or VCR.

Perhaps a technological measure is not “effective,” even if it functions properly, if access may be gained by means other than circumventing the device, that is, if the access device controls one “door” to a work, but another “door” exists and is not technologically locked, then locking only one “door” is not “effective.” See *Lexmark Int’l. v. Static Control Components, Inc.*, 387 F.3d 522 (6th Cir, 2004) (employing door metaphor) see discussion of DMCA, *infra*.

¹⁶ Information Society Directive, art. 6(3).

¹⁷ It is not clear that such a measure in fact does or will exist. Devices that control distribution come to mind, but in the digital environment, distribution (or making available) probably implies copying. For the same reasons, technological measures protecting the moral right of integrity will probably be covered by the EU’s definition of “effective.” By contrast, a technological measure that protects the attribution right might not. Moreover such a device would not necessarily be within the scope of WCT art. 12’s protection for copyright management information.

¹⁸ In the digital environment, many of the tasks publishers performed that were unrelated to the production and distribution of hard copies, such as promoting the works and accounting for sales, may be undertaken by agents or other new businesses whose compensation need not derive from owning the author’s copyrights. See, e.g., Jane Ginsburg, *Copyright and Control over New Technologies of Dissemination*, 101 *Colum. L. Rev.* 1613, 1645-47 (2001); Raymond Shih Ray Ku, *The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology*, 69 *U. Chi. L. Rev.* 263, 274-275 (2002).

(Berne Conv. art. 12), distributing of physical copies, including by means of rental (WCT art. 6), publicly communicating (Berne Conv. arts. 11, 11bis, 11ter, 14, 14bis; WCT art. 8), and against violations of the integrity and attribution rights (Berne Conv. art. 6bis) would all be covered.

But a particularly significant subset of technological protection measures addresses an arguably different act; these regulate access to a work of authorship.¹⁹ In the digital environment, works may be made available not only in traditional formats permitting unlimited access, but also in access-controlled formats that limit the user's apprehension of the work to a certain number of viewings or hearings, or to a certain time period. A technological measure shuts off access after the designated time period or number of consultations. The copy of the work may remain in the user's hard drive or on a CD Rom or similar external medium, but the user may be required to pay an additional fee or supply additional information before access will be restored. These sorts of formats may be particularly appealing to users who do not need or desire unlimited viewings or hearings of the work, assuming that a reduction in price accompanies the reduction in access. Whatever the business justifications for access controls, the question for interpretation of WCT art. 11 is whether it prohibits the circumvention of these measures as well.

Coverage of access controls: The response turns on whether access controls are "used by authors in connection with the exercise of their rights under the Treaty or the Berne Convention." We will consider, first, whether accessing a work comes within the Berne-WCT minimum rights. Next, we will address whether access controls are "used . . . in connection with" the exercise of those rights. In connection with the first question, it is important to distinguish accessing a *work* from accessing a *copy* of a work, as access controls generally apply to the former. Suppose a user purchases a CD ROM containing a copyrighted work, such as a videogame. She has acquired a copy, the physical medium in which the work is embodied. But the medium is not the work. The work is the videogame; to access this, she needs to load the game into her computer or videogame player; when the game's sounds are heard and the images appear on the screen, she will have accessed the work. If a technological measure included on the CD Rom does not permit her to play her copy of the game unless, for example, she enters a password, or plays the game only on certain designated computers, that is a measure controlling access to the work.

In light of this distinction, can it be said that the Berne Convention or WCT establish a right to control access to a work? The WCT introduces a right of distribution

¹⁹ For a description and analysis of technological protection measures, see, e.g., June Besek, *Anti-Circumvention Laws and Copyright: A Report From the Kernochan Center for Law, Media and the Arts*, 27 *Colum. J. L. & the Arts* 389, 446-66 (2004) [hereafter, Besek, *Anti-Circumvention Laws*]; Jeffrey Cunard, *Technological Protection of Copyrighted Works and Copyright Management Systems: A Brief Survey of the Landscape*, in *Adjuncts and Alternatives* 24; Jacques de Werra, *supra* note 25, at 200-205; Gillian Davies, *Technical Devices as a Solution to Private Copying*, in Irini Stamatudi and Paul Torremans, eds., *Copyright in the New Digital Environment*, 163, 173-78 (2000); Dean Marks and Bruce Turnbull, *Technical Protection Measures: The Intersection of Technology, Law and Commercial Licenses*, WIPO Workshop on Implementation Issues of the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT), Geneva December 6-7, 1999, WIPO Doc. WCT-WPPT/IMP/3.

of copies to the public, but this right addresses material (rather than electronic) copies; it would not extend beyond conferring a right to control access to a physical *copy*, rather than to a *work*.²⁰ The WCT also synthesizes the Berne Convention's various provisions on public performance into a general right of "communication to the public," including by digital delivery.²¹ This right would appear to cover "access" to a work through online media; it is considerably less clear that it would also cover subsequent apprehension of a work once the user downloads a copy to the user's storage medium, or once the user acquires a free-standing copy, such as a CD ROM.²² The subsequent acts may "perform" or "communicate" the works, but not in or to the public. Neither the Berne Convention nor the WCT requires member States to extend exclusive rights to private performances or communications.

Accessing a work expressed in digital form might nonetheless implicate the reproduction right under the Berne Convention: each apprehension of the work implies the creation of a temporary copy in the user's RAM. The reproduction right set out at Berne Conv. art. 9(1) extends to "any manner or form;" thus it may well cover temporary digital copies of this kind. But the scope of the reproduction right proved sufficiently controversial at the Diplomatic Conference that produced the WCT, so that many signatories to the WCT may not subscribe to a characterization of the scope of the reproduction right that would embrace a right of access to a work.

Given the continuing uncertainty in some quarters regarding the scope of the reproduction right, does it follow that WCT member States are not obliged to protect access controls against circumvention? Not necessarily, because one must next ask whether access controls are technological measures "used in connection with the exercise" of exclusive rights. Here the case for WCT coverage appears stronger. For example, access controls may be said to be used in connection with the exercise of the reproduction and communication rights, because an access-controlled copy, even if reproduced or communicated without authorization, will yield its copyist or recipient no benefits; that person will not be able to apprehend the work.²³ Thus, access controls underpin the reproduction, communication and distribution rights.

²⁰See WCT art. 6 and accompanying Agreed Statement.

²¹See *id.* art. 8 ("authors of literary or artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may *access* those works from a place and at a time individually chosen by them." Emphasis supplied.)

²²Article 6 of the 2001 European Union Information Society Directive, however, implements WCT art. 11 by protecting access controls.

²³See *Kabushiki Kaisha Sony Computer Entertainment v Stevens* [2003] FCAFC 157 (30 July 2003). In an action under section 116A of the Australian copyright act, which gives copyright owners a right of action against sellers of devices whose purpose is to circumvent technological protection measures, the court construed "technological protection measure" to include controls that block access to unauthorized copies because the controls "prevent or inhibit the infringement of copyright in a work." A technological measure that "renders the infringing copies . . . useless," meets the statutory requirement of preventing infringement "by rendering the sale of the copy 'impracticable or impossible by anticipatory action.'" This decision also exemplifies the uncertainty regarding the relationship of RAM copying to the reproduction right; two of three judges held that temporary storage in RAM did not produce a copy "in material form," and therefore no reproduction within the meaning of the Act had occurred.

Acts prohibited -- “the circumvention”: The WCT text appears most directly to cover the acts of removing, breaking or bypassing a technological measure. But relatively few individual users are likely to be able to engage in these acts unaided by a device that will overcome the protection. The question therefore arises whether the formulation “the circumvention” covers only that act, or also reaches the more economically significant activity of “preparatory acts,” including supplying a device that will enable the circumvention. The earlier version of art. 11 set out in the Basic Proposal²⁴ specifically targeted circumvention devices; should one infer from the final version’s more abstract expression a rejection of the liability of manufacturers and distributors of devices?²⁵

Such an inference seems unwarranted, because it would significantly diminish the effectiveness of the prohibition. First, limiting the prohibition to the act of circumvention would mean that copyright owners would need to discover and prove the commission of acts that may often occur in private, at the user’s home. This seems both difficult for copyright owners and undesirable to users.²⁶ Second, outlawing the device as well as the activity is likely to have a greater impact on the provision of circumvention devices; without the device, less circumvention is likely to occur, and it is more effective to pursue a small number of device suppliers than the large numbers of their customers.²⁷ Moreover, the formulation “the circumvention” should be read in the context of the sentence in which it appears. An interpretation that disfavors effective protection against circumvention by limiting the prohibited conduct to the sole act of circumvention, rather than encompassing the provision of devices as well, would be inconsistent with art. 11’s direction that member States “shall provide adequate legal protection and effective legal remedies against the circumvention . . .”²⁸

Acts prohibited – circumvention of technological measures “that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law”: Not all acts of circumvention are violations of article 11; member States incur no obligation to prohibit circumventions that allow the user to exploit a public domain work, or to engage in an act authorized by the right holder, or, more importantly, that allow the user to engage in a non infringing act, such as accessing a work in the public domain, or copying for purposes endorsed by articles 10 and 10bis. Article 11 delegates to member States’ laws the determination of permissible acts, but

²⁴ Basic Proposal for the Substantive Provisions of the Treaty on Certain Questions Concerning the Protection of Literary and Artistic Works to be Considered by the Diplomatic Conference, in 1996 Records at 217, WIPO Doc. CRNR/DC/4.

²⁵ See, e.g., Thomas C. Vijn, Copyright Imperilled? 21 EIPR 192, 201 (1999); Alain Strowel and Séverine Dusollier, Legal Protection of Technological Systems, Workshop on Implementation Issues of the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT), Geneva, December 6-7, 1999, WIPO Doc. WCT-WPPT/IMP/2 at 7, available at: http://www.wipo.int/documents/en/meetings/1999/wct_wppt/pdf/imp99_2.pdf. Contra, Kamiel Koelman, A Hard Nut to Crack: The Protection of Technological Measures, 22 EIPR 272, 273 (2000) (whether WCT art. 11 requires member States to prohibit the act of circumvention is “debatable”).

²⁶ See, e.g., Marks & Turnbull, *supra*, at 6 (pointing out privacy and practical concerns underlying the monitoring of private activity that a prohibition limited to the act of circumvention would entail).

²⁷ Accord, Reinbothe & von Lewinski, *supra*, at 144.

²⁸ Accord, *id.*, at 145; Ficsor, *supra*, at 549.

these must remain consonant with the scope of exceptions and limitations allowed under WCT art. 10 and Berne Conv. arts. 9(2), 10, 10bis, 11bis and 13.

The difficulty in implementing WCT article 11 arises with respect to the prohibition of circumvention devices and services. These may be used to engage in acts that infringe, but they may also be used for permitted purposes. If the prohibition sweeps too broadly, it may bar the manufacture and dissemination of devices or services that have legitimate uses other than to circumvent controls on access to copyrighted works. Too extensive a prohibition may frustrate whatever legitimate activities the devices may permit. Equally importantly, too broad a prohibition may hamper the development of useful new technologies. On the other hand, if national law provided that a device may be distributed so long as it is capable of being put to use for non infringing purposes, the prohibition would likely become meaningless. This in turn would put the national law in tension with article 11, for that law's protection of the technological measure would be neither "adequate" nor "effective."

For example, an access-circumvention device may be used to decrypt public domain motion pictures, but the same device can be employed to decrypt works still under copyright. A device that circumvents copy controls may be used to copy limited portions for purposes of illustration for teaching, but it may also be used to make unlimited complete copies to distribute to one's friends (or to the world over the Internet) for purposes of personal enjoyment. In most instances, and especially for mass-market devices, the maker or provider of the device will not know, at the time the device is made available, the nature of the use to which it will be put (although he or she might well anticipate that the market for the device is not likely to be limited to researchers, teachers and librarians).²⁹ Even if the device is designed in good faith to allow the public to decrypt DVDs of "The Sheik" or "Birth of a Nation" or other silent-era motion pictures in the public domain, it is equally capable, and probably more likely, to be used to unlock the digitized *oeuvre* of Federico Fellini or Woody Allen.

The Basic Proposal sought to address the problem of intended purpose or likely utilization by defining the prohibited device as one whose "primary purpose or effect" was to circumvent. This drew considerable opposition, however, notably from delegations who urged a "sole purpose or effect" standard.³⁰ The final version of article 11 avoids that controversy by declining to define targeted devices (indeed, not mentioning devices at all), and leaving it to member States to determine how to protect against "the circumvention . . ." As the analysis above suggests, however, the "adequate and effective" proviso would seem to require member States to bar the general circulation

²⁹ The context of the production or provision of the device may be determinative in certain circumstances. For example, if a university's information technology department supplies a circumvention device to university teaching or library staff for purposes of research or preservation, the uses of the device will likely be limited to those "permitted by law," and the provision of the device should therefore be permissible as well. Problems would arise, however, were the same device distributed to the general public, because the activities of the recipients of the device would no longer be likely to be confined to non infringing acts.

³⁰ See 1996 Records at 711-14; proposed amendment to substitute "sole intended purpose" for "primary purpose or effect" (submitted by Singapore), WIPO Doc. CRNR/DC/12 at 1996 Records 712, para. 526.

of circumvention devices. For the same reason, it also appears to disallow a “sole intended purpose” standard. While that standard might have proved too coarse a sieve, the opposite risk remains, that, in the absence of treaty guidance on the preservation of non infringing uses, national implementing laws will design so fine a mesh that too few non infringing applications will succeed in passing through. The challenge for national laws, then, is to determine how to regulate the creation and dissemination of circumvention devices without effectively cutting off the fair uses that at least some devices, in the right hands, would permit.

“Effective legal remedies”: WCT Article 11 does not instruct member States regarding the nature of the sanction for violating the anti circumvention norm. Thus, the WCT does not specify whether member States must grant injunctive relief against the distribution of circumvention devices or offering of circumvention services. In many cases, that relief may be necessary to insure “adequate and effective” protection, but there may be situations in which a lesser course, such as permitting the distribution of the device, subject to remunerating right owners, might be envisioned. As a general matter, the TRIPs provisions on the enforcement of intellectual property rights, arts. 41-61, indicate the range of remedies that constitute effective relief. It is worth noting that the WCT does not require that protections for technological measures be enacted as part of national copyright laws; that certainly is one route, but so too are sui generis laws, or inclusion of protections within the scope of more general laws, such as those addressing unfair competition.³¹

One matter, discussed in connection with the Basic Proposal, was whether member States should be obliged to impose design mandates on consumer equipment, so that mass market playback devices would interact successfully with technological protection measures applied to the content of the works played back. Mandates of this sort had been posited and debated as early as the WIPO Draft Model Law of 1990.³² But those debates occurred in the context of discussions over mandated protection measures, such as the Serial Copy Management System ultimately required for digital audio tape players by the 1992 US Audio Home Recording Act.³³ Once the drafters determined to leave the design of protection measures to the member States, design mandates were no longer at issue at the international level. Member States remain free to impose such requirements as a means of domestic implementation of the anti circumvention norm, but they have no duty to do so. The trend, in fact, is the other way: both the US and the EU have explicitly dispensed the designers of playback or other devices from having to

³¹ For example, Japan has divided coverage of technological measures between the copyright law and the unfair competition law. See Copyright Law (Law No.48, promulgated on May 6, 1970, as amended through June 12, 1988) Article 120bis(i); Unfair Competition Prevention Law (No. 47 of May 19, 1993, as last amended on April 23, 1999) – art. 2(x)-(xi), discussed in Besek, *Anti-Circumvention Laws*, supra, at 431-36. Australia has done this solely within the provisions of the *Copyright Act* 1968 (ss 116A and D) but makes them the subject of separate rights of action that may be brought by the copyright owner.

³² See Memorandum prepared for the Committee of Experts on a Draft Model Law, 1990 Copyright 279-80, para. 312-18; Report, id. at 299-300, para. 159-67.

³³ See id. at 279, para 309-10 (Memorandum); 300 para. 164 (Report); 17 USC sec. 1002.

comply with the specifications of the protection measure, so long as they do not circumvent it.³⁴ Non cooperation is fully permissible; aggressive hostilities are not.

We have considered the policy underlying WCT article 11; does the WCT successfully implement that policy? If the goal was to promote the digital distribution of works of authorship by giving authors some sense of security that copy or access-protected formats will not be vulnerable to piracy, it remains to be seen how effective national implementations of article 11 prove to be in preventing or forestalling circumvention³⁵ activities or devices. If the companion goal was to ensure that privileged unauthorized uses could continue to be made notwithstanding authors' resort to technological protections, it remains to be seen whether the various member State attempts to reconcile meaningful protection with preservation of copyright exceptions and limitations achieve a successful balance. With that caution in mind, we turn to the US experience in implementing the mandates of the WIPO Treaties.

II. The U.S. Experience with legal protection of technological protections of works of authorship

The following discussion will examine the text of Section 1201 of the 1976 Copyright Act and its judicial and administrative interpretation.³⁶ The text defines three new

³⁴ See 17 USC sec 1201(c) ("no mandate" clause); Information Society Directive, supra note 24, Recital 48.

³⁵ See, e.g., 17 U.S.C. sec. 1201(d)-(j); Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, art. 6(4), para. 43, Official Journal L 167, 22/06/2001.

³⁶ Section 1201 provides, in relevant part:

§ 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. . . .

(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—

violations: (a)(1) to circumvent technological protection measures that control access to copyrighted works; (a)(2) to manufacture, disseminate or offer, etc. devices or services, etc. that circumvent access controls; and (b) to manufacture, disseminate, or offer, etc. devices or services etc. that circumvent a technological measure that "effectively protects a right of the copyright owner" It is important to appreciate that these violations are distinct from copyright infringement. The violation occurs with the prohibited acts; it is not necessary to prove that the dissemination of circumvention devices resulted in specific infringements, or that the purpose of circumventing an access control was to commit an infringing act. On the other hand, section 1201 also sets out a long, disparate (and somewhat incoherent) list of exceptions to the prohibition on circumvention of access controls.³⁷ Section 1201 thus appears to expand the scope of copyright in the following ways:

1. It creates a claim for unauthorized access to works of authorship;
2. It makes distributors of circumvention devices directly liable for the dissemination of the means to gain unauthorized access;
3. It makes distributors of circumvention devices directly liable for the dissemination of the means to make copies or to engage in communications to the public;
4. It makes disseminators of both kinds of devices liable even if some of the end users to whom the devices are distributed would employ the devices for non infringing purposes.

To appreciate the actual scope of section 1201, it is necessary to inquire further into the subject matter of its protection, into the acts it prohibits, and into its accommodation of copyright exceptions. That inquiry will allow us better to assess whether section 1201, at least as experienced so far, has over-expanded the reach of copyright, or, rather, has enabled copyright to adapt to the challenges and opportunities that digital media present.

(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.

For a discussion of the legislative history of Section 1201, and of proposals that preceded it, see Besek, *Anti-Circumvention Laws* at 400-07 (2004).

³⁷ See 17 USC sec. 1201(d)-(j).

Subject matter protected: We have seen that section 1201 covers two different kinds of protective measures, those that “effectively control access to a work protected under this title [the Copyright Act],” and those that “effectively protect a right of a copyright owner,” i.e., that protect against copying and communicating to the public. Judicial decisions construing section 1201 have considered what it means to protect “effectively.” They also have addressed whether the object of the access control measure is a “work protected under this title.”

“Effectively protect:” With respect to the first issue, the courts are unanimous that “effective” protection does not mean protection that is especially difficult to crack.³⁸ For example, employing the door-and-key metaphor that judges addressing access issues seem to favor,³⁹ the court in *321 Studios v. MGM*, a case involving the sale of devices designed to permit “backup copying” of protected DVDs, quipped that the claim that the DVD protection code is not “effective” “is equivalent to a claim that, since it is easy to find skeleton keys on the black market, a deadbolt is not an effective lock to a door.” The door metaphor reappeared in a more serious challenge to the effectiveness of a “lockout code”’s protection in *Lexmark v. Static Controls Corp.*, a decision concerning the circumvention of a code controlling access to the functions of a printer. In that case, the Sixth Circuit Court of Appeals observed that the printer engine program was accessible by other means.

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 . . . it does not make sense to say that 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,” and it seems clear that this provision does not naturally extend to a technological

³⁸ *321 Studios v. MGM*, 307 F.Supp. 2d 1085, 1095 (ND Cal. 2004). See also *Universal Studios v. Reimerdes*, 111 F. Supp. 2d 346, 317-18 (SDNY 2000), *aff’d sub nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001) (rejecting as “spurious” the claim that DVD protection code did not “effectively” protect DVDs because a Norwegian teenager easily cracked it).

³⁹ See also *Pearl Indus. v. Standard I/O*, 275 F.Supp.2d 326, 350 (D. Me. 2003) (describing plaintiff’s access control measure as “the ‘electronic equivalent’ of a locked door”).

measure that restricts one form of access but leaves another route wide open.⁴⁰

The significance of the court's interpretation depends on how many works will come within the two elements of the described universe: 1. works whose use depends on interaction with a computer program that will function only on verification of an authentication sequence; 2. the code of that computer program can be seen or copied without going through the authentication process.⁴¹

Controlling access to a work of authorship: The *Lexmark* case is most significant for its analysis of the second issue -- whether the technological measure controls access to a work protected under the Copyright Act. In notorious, but happily short-lived, attempts to leverage the DMCA into protecting the "aftermarket" for spare and replacement parts, the producers of printers and cartridges, in one case, and of garage door openers in the other,⁴² asserted that rival printer cartridge and door opener manufacturers had violated the DMCA's prohibition on circumvention of access controls. In both cases, the spare part in question would not interact with the host device unless the host device recognized the spare part as authorized to function together with the host device. If the spare part entered the appropriate authentication sequence, or in the terms of another frequently-used metaphor, engaged in the "secret handshake" with the host device, then the host would be "fooled" into "thinking" that it was working with a component made by the same producer, and would allow the component to perform its intended function. The "secret handshake" thus made it possible for a rival printer cartridge to substitute for the printer producer's own replacement cartridges, and for a "universal garage door opener" to open the remote controlled garage doors installed by a rival company.

The question that should leap to mind is: "What have printer cartridges and garage doors to do with copyright?" Nothing, except, emphasized the plaintiffs, that computer programs control the functioning of these devices, and computer programs are copyrighted works. The dazzling (or mind-boggling) consequence of plaintiffs' reasoning: any object whose workings are controlled by computer programs -- and today, that means an endless variety of consumer and industrial goods -- can come within the scope of section 1201 if the object's producer makes access to those programs subject to an authentication sequence. As a policy matter, this is inconceivable. Among other things, Congress has persistently declined to legislate design protection, in part because

⁴⁰ 387 F.3d 522, 547 (6th Cir. 2004). The court also stated "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"; this proposition is questionable: the lock continues to control access to those who do not have keys.

⁴¹ There is a more radical, but less plausible, understanding of the court's characterization of otherwise accessible: as discussed earlier, the "work" is an incorporeal object, thus, a work distributed in digital copies which are access-protected, and in traditional hard copies which are not access-protected, is "otherwise accessible" without circumventing the digital copies, because recourse may be had to the hard copies. This would mean that section 1201(a) would apply only to technological protections of works made available only in digital protected copies. It seems unlikely that Congress, in seeking to encourage digital dissemination of works, also sought to discourage dissemination of the same works in traditional non protected formats. Indeed, such a construction could lead to the "digital lockup" that many critics of the DMCA have feared.

⁴² See *Chamberlain Group v. Skylink Technologies*, 381 F.3d 1178 (Fed. Cir. 2004).

of its inability to resolve the spare parts issue;⁴³ it would be extraordinary if it achieved the result of an exceptionally strong design protection regime through the stealthy means of the DMCA.

But does the *text* of section 1201 permit this result? The computer program that controls the functioning of the consumer product may indeed be a copyrighted work. The *Lexmark* court held that the authentication sequence was insufficiently original to be protectable, but the printer program was copyrightable. Nonetheless, that was not sufficient to bring the access control within the scope of section 1201. In a common sense interpretation of the text, the court reviewed earlier “secret handshake” cases, involving access to transmissions of recordings of musical works, to videogames, and to motion pictures on DVDs. The court underscored that all involved circumvention of access to computer programs that were “conduit[s] to protectable expression.”⁴⁴ In the printer cartridge case, by contrast, invocation of the computer program was clearly pretextual: operating the program did not make it possible to see, hear, or otherwise engage with a work of authorship. Rather, “the program’s output is purely functional: [it] ‘controls a number of operations’ in the Lexmark printer.”⁴⁵

Nature of the access that the measure controls: The court in the garage door opener case reached the same result, but for different reasons. Where the *Lexmark* court focused on the “work” that is the object of the access control, the *Chamberlain* court addressed the *purpose* of the access that the technological measure controls. The court interpolated into section 1201 a requirement that the protection against circumvention of an access control be related to protection against infringement. To the extent that access controls forestall infringement, for example, by making unauthorized copies unplayable, and therefore futile, the access control comes within the scope of section 1201. But, if the uses that the access control cuts off are not infringing uses, then the access control is not one that section 1201 was designed to protect, the court determined.⁴⁶ In the case of garage door openers, this makes some sense: using the opener does not infringe any copyrights. But, as applied to access controls that are “conduits” to works of authorship, the proposition is in some tension with Congress’ goals in prohibiting the circumvention of those technological measures. The *Chamberlain* court worried that interpreting section 1201 to create an independent violation for circumventing access controls (or disseminating access circumvention devices) would “effectively create two distinct copyright regimes,” one tied to the traditional rights of copyright owners (section 1201(b)), and the other allowing copyright owners “unlimited rights to hold circumventors liable under § 1201(a) merely for accessing that work, even if that access enabled only rights that the Copyright Act grants to the public.”⁴⁷

But there is considerable evidence from the text and from the legislative history

⁴³ The closest Congress has come so far is Chapter 13 of title 17, which sets out a *sui generis* regime limited to the protection of boat hull designs.

⁴⁴ 387 F.3d at 547-48.

⁴⁵ Id at 548.

⁴⁶ *Chamberlain v Skylink*, 381 F.3d at 1197-1201.

⁴⁷ Id. at 1200-01.

that Congress did intend to create an additional copyright regime, based on the control over access to digitally distributed works of authorship. The text indicates that the “access” that section 1201(a) protects goes beyond traditional copyright prerogatives; it distinguishes “access” from a “right of the copyright owner under this title.” Some activities subject to access controls do not implicate traditional copyright owner rights such as reproduction and public performance. For example, an access control may limit the number of viewings of a motion picture distributed on a DVD. But if the viewings occur at home, they likely do not come within the traditional scope of exclusive rights. Thus, suppose I purchase a time-loaded or limited-viewing DVD, for a lower price than an unlimited viewing DVD, and that I circumvent an access protection in order to obtain unlimited number of private viewings of the film for an unlimited time. I have not committed copyright infringement, because the public performance right does not reach the extra viewings. I have, however, defeated the purpose of offering the film on a pay-per-view or similar basis. The legislative history indicates that the DMCA was designed in part specifically to foster a variety of business models offering the public a diversity of levels of access, for a diversity of prices. As the House Commerce Committee reported:

[A]n increasing number of intellectual property works are being distributed using a “client-server” model, where the work is effectively “borrowed” by the user (e.g., infrequent users of expensive software purchase a certain number of uses, or viewers watch a movie on a pay-per-view basis). To operate in this new environment, content providers will need both the technology to make new uses possible and the legal framework to ensure they can protect their work from piracy.⁴⁸

“In other words,” my Columbia colleague June Besek has explained, “providing copyright owners with the ability to preclude unlimited access was a goal of the DMCA, not just an unforeseen and unfortunate consequence.”⁴⁹ This appears to be true, even when some of the precluded access would not result in copyright infringement.

Acts prohibited: Section 1201 prohibits the *act* of circumventing an access control, and the “*trafficking*” in devices that circumvent either access controls or “rights” controls. It does not prohibit the act of circumventing a rights control, in part because the results of that act will be directly infringing (or will qualify for an exception), and in part because the most economically significant act is the distribution of the device that will allow the end-user to circumvent. By contrast, circumvention of an access control does not directly result in an infringement. If circumvention of an access control is not unlawful, then, arguably, dissemination of a device that enables circumvention of an access control would not be wrongful either. By making the act of access circumvention unlawful, the DMCA lay a stronger foundation for prohibiting the dissemination of enabling devices as well.

⁴⁸H.R. REP. NO. 105-551, pt. 2, at 23 (1998).

⁴⁹Besek, *Anti-Circumvention Laws*, supra, at 474.

Circumvention: While most of the cases involve circumvention devices, a few cases have arisen concerning the act of circumvention.⁵⁰ One of these put in issue the meaning of “to circumvent.” In *IMS Inquiry Mgmt. Sys. v. Berkshire Info. Mgmt. Sys.*,⁵¹ Berkshire accessed IMS’s database by using a password apparently obtained from one of the IMS’s customers. Berkshire defended against the section 1201(a) claim on the ground that it did not break down the door of IMS’ database; it used an actual key. The court agreed: “Defendant did not surmount or puncture or evade any technological measure to [gain access]; instead, it used a password intentionally issued by plaintiff to another entity.”⁵² This interpretation is questionable. Section 1201(a)(3)(A) defines “to circumvent” as “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*” (emphasis supplied). Entry of the password “deactivates” the measure that restricts access;⁵³ if the password is employed by an unauthorized user, then the deactivation will not have occurred with the copyright owner’s authority.⁵⁴

Devices: Section 1201(a)(2) and (b) do not prohibit the dissemination of every device that *might* be used to defeat an access or rights control. These provisions do not target general purpose devices whose accidental, incidental or unwitting use results in circumvention. Nor does it bar those devices that, while capable of, and even used for, circumvention, are primarily designed or used for other purposes. The law prohibits the manufacture and trafficking in devices and services in the following three circumstances:

1. The device was "primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access" to a copyrighted work or “effectively protects a right of the copyright owner”; or
2. The device albeit not *primarily* designed to circumvent, in fact "has only limited commercially significant purpose or use other than to circumvent . . ."; or
3. The device is "marketed" (i.e., advertised or promoted) as a device to be used to circumvent access or rights controls. In this case, the target of the law is the person

⁵⁰ In one case, the plaintiff brought an action seeking a declaratory judgment that the section 1201(a)(1) was unconstitutional because it restrained his First Amendment right to reverse engineer software that blocked access to certain Internet sites, in order to publish a list of the blocked sites. The court held the complaint too vague to give rise to an adjudicable “case or controversy.” See *Edelman v. N2H2*, 263 F.Supp.2d 137 (D. Ma. 2003). In any event, it is likely plaintiff’s conduct would have benefited from statutory and administrative exceptions to sec. 1201(a). See Besek, *Anti-Circumvention Laws* at 414-15.

⁵¹ 307 F.Supp.2d 521 (SDNY 2003).

⁵² *Id.* at 533.

⁵³ A password-controlled access measure fits the statutory definition of a technological measure that effectively controls access to a work, see 17 USC sec. 1201(a)(3)(B).

⁵⁴ See, e.g., *321 Studios v. MGM*, 307 F.Supp. 2d 1085, 1098 (N.D. Cal. 2004) (“321 states that its software does not avoid, bypass, remove, deactivate, or otherwise impair a technological measure, but that it simply uses the authorized key to unlock the encryption. However, while 321’s software does use the authorized key to access the DVD, it does not have authority to use this key, as licensed DVD players do, and it therefore avoids and bypasses [the] CSS [access control].”).

promoting the circumventing use; it is not the manufacturer or distributor of the device, unless that person acts in concert with the marketer.

Many of the cases that have arisen have involved rather obvious circumvention devices, such as cable and satellite descramblers,⁵⁵ and devices designed to neutralize the access controls on DVDs.⁵⁶ As a result, they have not required courts to determine whether the primary purpose or actual use of the device was to circumvent.⁵⁷ Courts have interpreted the text of section 1201 to reach trafficking in circumvention devices regardless of whether the circumventions that the devices enable would result in infringements. Thus, for example, in one of the DVD cases, *321 Studios v. MGM*, the court stated:

a simple reading of the statute makes it clear that its prohibition applies to the manufacturing, trafficking in and making of devices that would circumvent encryption technology, not to the users of such technology. It is the technology itself at issue, not the uses to which the copyrighted material may be put. This Court finds . . . that legal downstream use of the copyrighted material by customers is not a defense to the software manufacturer's violation of the provisions of § 1201(b)(1).⁵⁸

In most of the cases, nonetheless, the relationship between the circumvention that the device enabled and infringement was fairly apparent. For example, in one of the first cases decided under sec. 1201, *RealNetworks v. Streambox*,⁵⁹ the defendant's device imitated the "secret handshake" giving access to recorded music transmitted from the RealNetworks server. Unlike a Real Player, through which a customer could listen to the transmissions, but not copy them, the defendant's system ignored the Real server's "copy switch," enabling its customers to make unauthorized copies of the recorded music. In *321 Studios v. MGM*, the access circumvention device allegedly allowed users to make playable "backup copies" of DVDs that they had purchased, but there is no general copyright exception permitting the creation of "backup copies."⁶⁰ Moreover, protestations that the device simply facilitated lawful uses lost credibility in light of 321's "spam" promotion of the device under the slogan "Never buy another DVD again!"⁶¹

⁵⁵ See, e.g., *DirecTV v. Borrow*, 2005 US Dist LEXIS 1328 (N.D. Ill. 2005); *Comcast of Ill. v. Hightech Electronics*, 2004 US Dist LEXIS 14619 (N.D. Ill. 2004); *DirecTV v. Ferguson*, 328 F.Supp2d 904 (N.D. Ind. 2004).

⁵⁶ See, e.g., *Universal Studios v. Corley*, 273 F.3d 429 (2d Cir. 2001); *321 Studios v. MGM*, 307 F.Supp. 2d 1085 (N.D. Cal. 2004).

⁵⁷ An exception is *DirecTV v. Little*, 2004 US Dist LEXIS 16350 (N.D. Cal. 2004) in which the court determined that there was a factual dispute concerning whether the defendant's "smart cards" were "primarily designed for signal theft."

⁵⁸ 307 F.Supp. at 1097-98, *citing* *Universal Studios v. Corley*, 273 F.3d 429, 443 (2d Cir. 2001) and *US v. Elcom*, 203 F.Supp.2d 1111, 1120 (ND Cal. 2002).

⁵⁹ No. C99-2070P, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. Jan. 18, 2000).

⁶⁰ 17 USC sec. 117 permits archival copying of computer programs, but not every work expressed in 1s and 0s is a "computer program." See generally *US v. Elcom*, *supra*, at 1135.

⁶¹ A copy of the "spam" was forwarded to me three years ago, with the inquiry, "Can they do that?"

Similarly, although the US distributors of the Norwegian-authored “De-CSS” DVD access-circumvention program claimed the program could be used in a Linux-based DVD player, the program was not distributed in the US as a component of such a player;⁶² rather it was made available as a free-standing program which could be used to neutralize the access protection on unauthorized copies of DVDs run on Windows players. It doubtless did not assist defendants’ cause to have published the code in an online magazine called *2600.com, the Hacker Quarterly*. As the district court observed with some relish, “*The Hacker Quarterly* has included articles on such topics as how to steal an Internet domain name, access other people’s e-mail, intercept cellular phone calls, and break into the computer systems at Costco stores and Federal Express.”⁶³

A more debatable condemnation of an access-circumvention device occurred in another early case, *Sony Computer Ent. v. Gamemasters*.⁶⁴ Defendants sold a “Game Enhancer” device that allowed users to alter the real-time play of a videogame (without preserving the modifications), and that also allowed users to override Sony’s “region coding,” so that a game purchased in a differently-coded region, such as Europe or Japan, could nonetheless be played on a US PlayStation console. Sony also claimed that the device that overrode the region-coding also made it possible to play counterfeit copies of PlayStation games, but little evidence supported this contention. The court granted a preliminary injunction on the ground that defendant’s device neutralized an access control; the court did not inquire into whether a game lawfully acquired in one region could be played in another without infringing copyright. Both the “first sale” (or “exhaustion”) doctrine,⁶⁵ and the confinement of the performance right to *public* performances, however, suggest that the copyright owner’s exclusive rights do not extend to determining the geographical zones in which members of the public may privately view copies lawfully made. Applying section 1201(a) to protect against circumvention of access measures that limit those copies to playback devices licensed for a given territory thus results in a scope of protection not otherwise available under the copyright act.

But if region-coding is obnoxious, cannot much the same objection be made regarding access measures that control pay per view and similar schemes based on price discrimination? The answer may turn on the existence of evidence that Congress sought to protect the latter business models, while similar evidence does not appear to exist regarding the former. Moreover, the latter business models are built on a quid-pro-quo: the extent of access allowed turns on the price the consumer pays. Price discrimination does not appear to characterize region-coding; the consumer is not offered world-wide access at one price, and geographically restricted access at a different, lower, price. These responses do not, however, contradict the basic observation that, by protecting against the circumvention of access controls, without further requiring proof of a nexus between the circumvention and infringement, Congress has permitted, indeed encouraged, copyright owners to create and control markets for their works that the traditional exclusive rights under copyright would not secure. Whether this is a good

⁶² This might have been permissible under section 1201(f).

⁶³ *Universal Studios v. Reimerdes*, 111 F.Supp.2d 294, 308-09 (SDNY 2000) (citations omitted).

⁶⁴ 87 F.Supp.2d 976 (N.D. Cal. 1999).

⁶⁵ See 17 USC sec. 109(a).

thing or a bad thing may depend on whether, overall, more works become available to more consumers, under a greater variety of terms, conditions, and prices, than were available without legally protected technological protection measures.

Accommodation of copyright exceptions: Even so, there is another trade-off to consider. Is this flourishing of new owner-controlled copyright markets compatible with the various exceptions that limit the reach of copyright law in a variety of circumstances? Do we get more works for less money, but less freedom to quote from, teach from, build on, study, criticize and even ridicule them? To assess the impact on copyright exceptions of legal protection for technological protection measures, we have first to distinguish section 1201's treatment of circumvention of rights controls from that of access controls. With respect to access controls, section 1201 reaches both the end-users who directly circumvent those controls, and the persons who manufacture, distribute and market devices primarily designed or used to circumvent those controls. On the other hand, section 1201 includes several exceptions to these prohibitions. As construed by the courts, do these adequately accommodate desirable, albeit unauthorized, uses of copyrighted works?

With respect to rights controls, section 1201 does not reach end users who directly circumvent rights controls, or who employ devices to effect the circumvention. Thus an end-user who circumvents a copy control, and then makes a copy or communication permissible under the fair use doctrine or other applicable exception, is liable neither for a circumvention violation, nor for copyright infringement. An end-user who circumvents a copy control to make an unexcused copy or communication to the public will not be liable for a circumvention violation, but will be liable for copyright infringement. On the other hand, the prohibition on trafficking in rights control circumvention devices may make it difficult for many end-users to obtain and utilize the devices regardless of the purpose to which they would put them. Does the prohibition on distribution of devices primarily designed or used to circumvent rights controls therefore stifle copyright exceptions, and the beneficial uses those exceptions foster?

Exceptions to circumvention of access controls: The DMCA provides a variety of exceptions, including for reverse engineering, encryption research, and security testing.⁶⁶ Two decisions have construed the scope of the section 1201(f) exception for reverse engineering.⁶⁷ Both have found the exception inapplicable on the ground that the

⁶⁶ For a fuller description of these, and the other, exceptions to 1201(a), see, e.g., Jane C. Ginsburg, Copyright Legislation for the "Digital Millennium," 23 Colum.-VLA J. L. & the Arts 137, 148-52 (1999).

⁶⁷ Section 1201(f) provides:

(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.

defendants had not circumvented access controls for the sole purpose of creating non infringing interoperable programs. Rather, the defendants, having gained access by reverse engineering the plaintiff's control program, made infringing copies of the plaintiff's work. In *Storage Technology Corp. v. Custom Hardware Engineering & Consulting*,⁶⁸ the court held that while the defendant reverse engineered plaintiff's library maintenance program in order to break the access code, the defendant then simply copied the entirety of plaintiff's program.

In *Davidson & Assoc. v. Internet Gateway*,⁶⁹ the defendants broke the access code of the Battle.net online videogame service, in order to develop a Battle.net "emulation site" that would allow owners of copies of the Blizzard videogame to play their games online, without the advertisements and use restrictions imposed by the Battle.net site. Battle.net required users to enter an authentication sequence that would permit the website to verify that the user's copy of the game was authorized. Thus, Battle.net screened out unauthorized copies, and did not allow them access to the game site. Defendants' "bnetd" alternative site did not require users to enter the authentication sequence; as a result, owners of "counterfeit" copies could join in a multiplayer game environment that replicated the desirable aspects of the Battle.net experience. The court held that the output of the "bnetd" program infringed that of the Battle.net program because there were "no differences between Battle.net and the bnetd emulator from the standpoint of a user who is actually playing the game."⁷⁰

It is not entirely clear that the defendant's use in that case in fact exceeded the scope of the reverse engineering exception. Assuming the defendant had lawfully obtained a copy of the Blizzard and/or Battlenet programs, it appears to have accessed the program's code "for the sole purpose of identifying and analyzing those elements of the (Battle.net) program that are necessary to achieve interoperability of an independently created computer program (bnetd) with other programs (its users' copies of Blizzard)." Defendant was entitled to do this "to the extent any such acts of identification and analysis do not constitute infringement under this title." The decision does not demonstrate that the

(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.

⁶⁸ 2004 US Dist LEXIS 12391 (D. Mass. 2004).

⁶⁹ 334 F.Supp.2d 1164 (ED Mo. 2004).

⁷⁰ Id. at 1185.

defendant's *analysis* was infringing; rather, the *results* of the analysis may have produced a program too similar to the plaintiff's. On the other hand, the exception would not make very much sense if it did not take into account whether the program that results from accessing and studying the plaintiff's code is infringing. The caselaw developing a fair use exception for reverse engineering, for example, assesses whether the result of the reverse engineering is an independent non infringing program (similar in functionality but not expression).⁷¹ Moreover, the court's decision is generally consistent with the rationale for protecting access controls in the first place: to render unauthorized copies useless because the access control will not permit the copies to be viewed or otherwise enjoyed. In this case, the Battle.net authentication sequence rendered unauthorized copies of Blizzard relatively useless, because they would not be admitted to the online multiplayer site. Defendant's bnetd site allowed those copies to be played, thus defeating the purpose of the access control.

Copyright Office rulemaking: While the exceptions to section 1201(a) are multiple, they are also very narrowly defined, and do not admit of expansive judicial construction.⁷² As a result, Congress instructed the Librarian of Congress, in consultation with the Register of Copyrights, to conduct a rulemaking every three years to identify particular classes of works whose users would be "adversely affected by the prohibition . . . in their ability to make noninfringing uses under this title" and to suspend the application of the prohibition on the act of access control circumvention as to those works until the next rulemaking period.⁷³ Each rulemaking is *de novo*: a class identified in a prior rulemaking is not automatically reinstated; the Copyright Office must determine whether a need for an exemption still exists. It is important to recognize, however, that the prohibitions against trafficking in access circumvention devices continue to apply. Two rulemakings have now been conducted, and the following classes of works declared:

"compilations consisting of lists of websites blocked by filtering software applications" (first and second rulemakings);

"literary works, including software and databases, protected by access control mechanisms that fail to permit access because of malfunction, damage or obsolescence" (first rulemaking);

"Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete" (second rulemaking);

"Computer programs and video games distributed in formats that have become obsolete and which require the original media or hardware as a condition of access" (second rulemaking)

"Literary works distributed in e-book format when all existing e-book editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling of the e-book's read-aloud function and that prevent the

⁷¹ See, .e.g., *Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992); *Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596 (9th Cir. 2000).

⁷² See 17 USC sec. 1201(a)(1)(B)-(E).

⁷³ For a fuller discussion, see Besek, *Anti-Circumvention Laws* at 416-23.

enabling of screen readers to render the text into a ‘specialized format’” (second rulemaking).⁷⁴

The characteristic most of these categories share is obsolescence or malfunction: the work was made available in formats no longer generally in use or which are defective, and circumvention is necessary to access the work. The lists of blocked websites, or “Net Nanny,” exemption is different in kind, for, rather than protecting consumer interests regarding the ordinary use of defective or obsolete goods, it promotes free speech interests. The problem arises from software filters designed, for example, to protect children by blocking access to websites containing sex and/or violence, hence the term “Net Nanny.” Some of these filters may be over-exuberant in their coverage, and may screen out websites that are neither pornographic nor sadistic, but that may contain human anatomical references in medical or other educational contexts. The blocking programs include lists of the forbidden sites, but the list is encrypted. A third party seeking to determine whether a site has been wrongly targeted for exclusion cannot find out who is on the “black list” without decrypting the list. The Copyright Office was persuaded that an exception to the access control prohibition was needed to correct this problem.

As may be inferred from the specificity of the exceptions resulting from the triennial rulemakings, these administrative proceedings do not present an opportunity to devise sweeping exceptions in the name of free expression, advancement of research, or other salutary goals. In significant measure, this is because Congress left the Library of Congress and the Copyright Office rather little room to maneuver. The EU Information Society Directive’s art. 12.1 instruction to the Commission to examine and report on a triennial basis “whether acts which are permitted by law are being adversely affected by the use of effective technological measures” may produce broader accommodations than the Copyright Office has been able to achieve in light of its far narrower statutory mandate. Another reason for the parsimonious nature of the Copyright Office classes of exempted works nonetheless bears emphasis: the Copyright Office also rejected a variety of more broadly-phrased classes because those urging the broader classes failed to produce significant evidence that users were now, or in the next three years would likely be “adversely affected by the prohibition . . . in their ability to make noninfringing uses” of access-protected works. The Copyright Office received many submissions detailing fears of “digital lockup” (as well as many submissions deploring copyright in general), but too little in the way of concrete demonstration that noninfringing uses were compromised.

Other authority for broader exemptions? The statutory scheme similarly constrains judicial authority to devise general exceptions to circumvention prohibitions. The array of specific exceptions makes inference of a general exception inappropriate. Moreover,

⁷⁴ Exemption to the Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64556, 64561 (proposed Oct. 27, 2000) (to be codified at 37 C.F.R. pt. 201); Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 68 Fed. Reg. 62,011 (Oct. 31, 2003) (to be codified at 37 C.F.R. pt. 201).

the delegation to the Copyright Office to designate circumventable classes of works suggests that Congress intended administrative rather than judicial proceedings to make the scheme more responsive to user needs not already specified in the statute. But, assuming Congress intended to foreclose judges from engrafting a general fair use type exception onto section 1201, may it do so, consistently with constitutional protections for the free speech interests that section 1201 arguably frustrates? In the absence of fair use, does the first amendment require invalidating section 1201 as an undue burden on protected speech?

Some litigants have asserted the unconstitutionality of the US Copyright Act's anticircumvention provisions. They have contended that fair use is constitutionally mandated, and that section 1201 "eliminates fair use." As a result, Congress would not have power to preclude fair use defenses to circumvention. Alternatively, they have argued that section 1201 suppresses speech – the speech in this instance is the DVD access-circumvention program De-CSS – and therefore violates the first amendment. Every court that has so far encountered these challenges has rejected them.⁷⁵ With regard to the first amendment, courts have observed that computer programs are a form of speech, but they are also functional. To the extent the government regulates the software's functional aspects, the law is "content neutral" as to the speech aspects. The law will not be considered to violate the first amendment if the regulation advances a legitimate government interest, and is reasonably tailored to achieve that purpose. Congress' interest was in promoting electronic commerce in copyrighted works, and Congress could legitimately seek to achieve this objective by making the distribution of circumvention devices unlawful.⁷⁶ The fair use assertions fared no better. First, courts expressed some skepticism as to whether fair use was constitutionally required. Even granting that fair use plays an important, first amendment-friendly role in balancing the rights of copyright owners against subsequent speakers, the courts have uniformly spurned the "extravagant claim" that section 1201 "unconstitutionally 'eliminates fair use.'"⁷⁷ The courts have observed that unprotected copies in non digital media remained available for all the usual fair use purposes, including by means of analog copying. Even copying from protected media, such as DVDs, might be rendered more cumbersome, but it was not completely foreclosed. The courts emphasized that "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."⁷⁸ And "Defendant has cited no authority which guarantees a fair user the right to the most technologically convenient way to engage in fair use. The existing authorities have rejected that argument."⁷⁹ The courts' rather abrupt treatment of the question probably reflects the contexts in which the cases arose, as much as the merits of a claim of entitlement to maximally convenient fair use. The cases have involved entrepreneurs and intermediaries who distributed circumvention devices that were perceived to facilitate piracy of DVDs and e-books. None of these intermediaries claimed to be engaging in fair use of the circumvented

⁷⁵ See *Universal v. Corley*, supra; *US v. Elcom*, supra; *321 Studios v. MGM*, supra.

⁷⁶ See, e.g., *Universal v. Corley*, 273 F.3d at 453-58; *Elcom*, 203 F.Supp.2d at 1127-37.

⁷⁷ *Corley* at 458.

⁷⁸ *Id* at 459.

⁷⁹ *US v Elcom*, 203 F.Supp.2d at 1131.

works; nor did they show that their customers in fact sought the devices primarily in order to engage in non infringing uses of the playable copies of DVDs that the devices enabled. Fair use in this context seemed primarily pretextual. But the concerns about convenience are not frivolous: at some point, particularly if analog or unprotected versions cease to be readily available, “inconvenient” may look more like “impossible.” Should such a dismal future appear more imminent, it may well be appropriate to reconsider the scope of the circumvention prohibitions. But we are a long way yet from that dire outcome.

Conclusion

Section 1201 does represent a rebalancing of power between copyright owners and users. But we should not immediately assume that any change in the prior state of affairs is a bad thing. After all, which prior “balance” do we mean? The one in which technology did not offer much potential for consumptive copying and copyright owners controlled access by controlling communications to the public? Or the one in which technology enabled widespread copying, but did not afford adequate and reasonable means of preventing or charging for the copying? Or the one in which technology permits massive copying, but also enables copyright owners to be paid for it? Or one in which technology enables copyright owners to prevent or frustrate copying? Taking the last pre-DMCA balance as somehow normatively compelled ignores the reality that copyright “balances” are highly contingent and contextual. The more useful question is, regardless of past allocations of power, whether the new balance makes sense for authors, owners, and users.

As a recently published 3-year study conducted by Columbia Law School’s Kernochan Center for Law, Media and the Arts concluded:

§ 1201. . . involves genuine tradeoffs: Congress made a judgment that technological protection would foster innovation in new content delivery mechanisms in order to provide consumers with a range of new options for experiencing copyrighted works, recognizing that technological controls might diminish the convenience of non-infringing uses. So far, the balance that Congress struck appears justified. Section 1201 has provided substantial benefits to consumers by encouraging the development of innovative new business models for delivering sound recordings, motion pictures, books and other copyrighted works to consumers.

On the other hand, there is little evidence at this point that technological controls are preventing privileged uses. Flexibility in the law, the realities of the digital environment and market imperatives appear to be accommodating legitimate uses. Most copyrighted works

are available for fair uses, though not necessarily in a form amenable to the most technologically advanced forms of copying, remanipulation and retransmission. Such limitations, however, are at the heart of the new business models that are emerging in the marketplace.

The reasons that DMCA critics offer for overhauling or replacing § 1201 are essentially the same ones presented to Congress in opposition to the legislation when it was under consideration. Congress took them into account in crafting § 1201. Based on the track record so far, § 1201 appears to be performing largely as Congress had envisioned and should not be overhauled or replaced. The benefits—more works available to consumers at a variety of price and convenience points—are real, and the costs have so far been manageable. It is important to continue to monitor § 1201's effects and, where problems become apparent, develop specific, focused solutions. At the present time, however, we should allow the new business models enabled by § 1201 the opportunity to continue to flourish.⁸⁰

I close on an optimistic note. This analysis has addressed the occasionally competing concerns of copyright owners and of users. The word “copyright owner” more often than not evokes a large, unloveable, multinational (or American), corporate entrepreneur, in short, an Evil Troll. It is easy to deplore technological protections if one thinks of them only in those apocalyptic terms. But one might instead focus on the opportunities technological protections extend to individual authors to disseminate their works, and to condition further copying or exploitation on remunerating the creators. Digital media, by making the means of production and dissemination available to any computer-equipped author, give authors a realistic opportunity to bring their works to the public without having to put themselves in thrall to traditional intermediaries. The technological measures that reinforce legal control may enable and encourage authorial entrepreneurship, because authors may be able to rely on these measures to secure the distribution of and payment for their works, and new business models may therefore emerge. Shifting control from publisher-trolls to authors not only enhances the moral appeal of the exercise of copyright, it also may offer the public an increased quantity and variety of works of authorship, as authors whom the traditional intermediary-controlled distribution system may have excluded now or soon may directly propose to the public (and be compensated for) their creations.

⁸⁰ Besek, *Anti-Circumvention Laws*, at 512-13