A Proposal in Hindsight: Restoring Copyright's Delicate Balance by Reworking 17 U.S.C. § 1201

Daniel S. Hurwitz

Introduction

The anticircumvention provisions enacted in 17 U.S.C. § 1201[1] as part of the Digital Millennium Copyright Act[2] represent an ambitious attempt by Congress to incorporate new technological realities into traditional copyright protection. While the statute was structured to be forward-looking and enable copyright law to take into account unforeseeable technological change, it suffers from numerous flaws.

Specifically, § 1201 enlarges the scope of copyright to an unprecedented degree, severely restricting the public domain;[3] it similarly risks gutting the fair use doctrine;[4] it potentially stifles innovation in both the creation of new media products and the invention of new technologies;[5] it wrests control of the development of copyright doctrine away from Congress;[6] and it actually manages to under-protect copyright holders in some key ways.[7]

In Part I of this paper, the development and structure of § 1201 as it currently stands are examined. Part II of this paper presents this author's proposed redrafting of the statute, addressing each of the aforementioned concerns.

---

[1] 17 U.S.C. § 1201 (2004).

[2] Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C.).

[3] *See infra* Part II.B.

[4] *See infra* Part II.C.

[5] *See infra* Part II.D.

[6] *See infra* Part II.E.

[7] *See infra* Part II.F.

PART I: HOW WE GOT HERE

Before the 1990s, copyright law as embodied in Title 17 of the United States Code was remarkably coherent. Under the Copyright Act of 1976,[8] writers and artists enjoyed basic, enumerated rights in their works[9] as soon as they were recorded in a tangible medium of expression[10] without having to jump through any administrative hoops (such as registration and notice requirements).[11]

Users' and consumers' rights were similarly well-defined: if one wanted to consume a copyrighted work, he paid for a copy (or borrowed one from a library) or he bought a ticket to a performance.[12] Even the fair use doctrine was intuitive enough that the average person knew what it entailed most of the time.[13]

Infringement cases were most commonly brought against those who sought to profit en masse from producing or trafficking in pirated goods,[14] not the individual who taped a buddy's LP. This was because it was impractical to pursue individual transgressors who deprived a copyright holder of only one sale, and by controlling the professional-grade duplication equipment and the master copies, copyright holders controlled the only means of getting top-quality copies of their works.[15]

The case of the VCR is illustrative of the status of copyright law before the 1990s. When Sony's Betamax player/recorder first debuted in the 1970s, enabling home recording of television broadcasts and fast-forwarding through commercials, "Motion Picture Association of America (MPAA) president Jack Valenti told the House Judiciary committee that 'the growing and dangerous intrusion of this new technology' threatened his entire industry's 'economic vitality and future security.'"[16] When Congress chose not to take action, MPAA constituents Universal Studios and Disney filed suit against Sony, claiming the Betamax machine "contributorily infringed" on their copyrights.[17] The United States Supreme Court held that private, non-commercial copies

---

[8] Copyright Act of 1976, 17 U.S.C. §§ 101-810 (2004).

[9] 17 U.S.C. § 106 (2004).

[10] 17 U.S.C. § 102 (2004).

[11] 17 U.S.C. § 408 (2004) (registration); 17 U.S.C. § 401 (2004) (notice).

[12] *See* http://www.respectcopyrights.org/content.html.

[13] 17 U.S.C. §107 (2004) (codifying the fair use doctrine); *see* http://www.whatiscopyright.org/.

[14] Rick Harbaugh & Rahul Khemka, *Does Copyright Enforcement Encourage Piracy?* 2 (Claremont Colleges Working Paper in Economics, 2001) *available at* http://econ.mckenna.edu/papers/2000-14.pdf.

[15] *Id* at 2. Or they licensed or sold their works to those who maintained that control. *Id.*

[16] DCC Report, *infra* note 20, at 21.

[17] 17 Sony Corp. of Am. v. Universal Studios, Inc., 464 U.S. 417 (1984).

made for home use constituted "fair use,"[18] and that such a substantial noninfringing use barred an action for contributory infringement.[19] Thus was born both the standard definition of "fair" home recording, and the consumer expectations that copyrighted works could sometimes be acquired legally without a direct purchase.[20]

The World of the Nineties

Then copyright law became confused – and quickly – in the 1990s. Several parallel developments made the copyright picture much more complicated. These were the digital revolution, the development of the internet (which produced the so-called "digital dilemma"), and the increased globalization of the American media.

The Digital Revolution

The digital revolution refers to the change in media that occurred once computer technology enabled the conversion of written text, two-dimensional visual art, audiovisual works, and phonograms into binary code.[21] This meant that perfect copies of works could be made, not only from the master copy, mold, or printing press, but using any other digital copy as a source.[22]

This is because of the nature of digital works – they are encoded in simple ones and zeroes (more accurately, signals to digital media read-

---

[18] *Id.* at 449-450.

[19] *Id.* at 442.

[20] The Digital Connections Council of the Committee for Economic Development [hereinafter "the DCC"], a Washington think-tank that makes commercial and policy recommendations for the betterment of the economy, recently released a report which describes the lasting effects of the *Sony* decision:

> The Sony decision has created a powerful presumption that private noncommercial copying of content is fair. Beyond its legal implications, the Sony decision, and the experience of users with copy-protected software (and, indeed, software in general) has created a consumer expectation that noncommercial copying for backup purposes, or to time-shift or space-shift (to use at a different time or in a different device), is acceptable. The VCR story illustrates how consumer expectations about a technology develop. Most consumers now expect that they can make a personal copy of software in order to have a backup or for time- or space-shifting purposes. Polls show that many people do not consider such copying wrong or believe that personal copying (as opposed to commercial copying) has a real impact on copyright owners.

"Promoting Innovation and Economic Growth: The Special Problem of Digital Intellectual Property – A Report by the Digital Connections Council of the Committee for Economic Development" [hereinafter "DCC report"] at 21, *available at* http://www.ced.org/docs/report/report_dcc.pdf (March 2004). The DCC Report details how these consumer expectations impact fair use inquiries. *Id.*

[21] *See generally* http://history.acusd.edu/gen/recording/digital.html (last modified May 5, 2004).

[22] http://www.respectcopyrights.org/content.html

ers to turn an electrical signal "on" or "off") and contain within the nature of their code the "DNA" needed to make an exact copy.[23] While the quality of the digital work depends on the process or equipment used to initially encode it, once encoded, the same binary code that gets decoded to read, see or hear the work tells copying equipment *exactly* how to construct a duplicate.[24]

The surreptitious infringer no longer had to face a choice between purchasing "professional-grade" original, or acquiring a somewhat degraded, illegal copy for free or relatively cheaply. Now, all that stood between paying and stealing was one's own morality and the knowledge of the existence of copyright law.

The benefits of the digital age are also astounding. The ability to transmit, without degradation, an entire work via wire or broadcast saves considerable money.[25] The digitally encoded media is easily manipulated, edited, or changed by its creator.[26] And the coded works can be encrypted so that only equipment or software applications that meet certain requirements (which can be contractually set by the copyright holders and equipment manufacturers) can access the encoded works.[27]

DVD As a Case Study[28]

A concrete example is useful to illustrate the digital revolution. Following the tremendous popularity and success of music distributed via the compact disc ("CD") medium, movie studios began in the 1990s to experiment with similar means of distributing high quality recordings

[23] *Id.* In fact, making a digital copy from a digital master is known as "cloning." *See* http://www.9to5computer.com/Hard-drive-duplicators-Clone-Card-faqs.htm.

[24] *See* http://www.9to5computer.com/Hard-drive-duplicators-Clone-Card-faqs.htm. In contrast, in the analog world, where a certain quantum of electromagnetic wavelength, colored dye, ink, or depth of groove on a record, etc., translates directly to the perceived quality of the work fixed within the medium, a copy reproduced from an existing copy always loses some quality. "Is Analog Harder to Copy?" *available at* http://www.publicknowledge.org/resources/tutorials/analog.

[25] The potential cost savings to distributors of copyrighted material alone are astounding – transmission of digitally encoded works allows hard copies to be produced, at least in theory, much closer to major distribution centers, meaning most of the weight of the final products need not be shipped great distances at all. Master recordings of radio and television programs need not get lost or broken en route to the broadcaster, and digitally equipped cinemas need not even care for reels of celluloid film. Tan Ching Yee, Remarks at the Launch of IDA-MDA Digital Cinema Effort (Nov. 19, 2003), *available at* http://www.ewcinemas.com.sg/Web/Promotion/ digitalcine mas/speech02.html.

[26] JoAnne E. Davies, *Advantages of Digital Media, at* http://www.quasar.ualberta.ca/edpy485/mmedia/advant.htm (last modified: May 16, 2000).

[27] See discussion of CSS, *infra*, at n. 32.

[28] This discussion borrows heavily from Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 308-310 (S.D.N.Y. 2000).

of theatrical films and television shows that took advantage of digital compression schemes to deliver better picture and sound than any format had previously allowed.[29] Borrowing from the tremendous success of the CD, the physical medium chosen for distribution of these digitally-encoded audiovisual works was the 5-inch, plastic Digital Versatile (originally, "Video") Disc, or DVD.[30]

However, with home CD burners already widely available, studios feared widespread piracy of motion pictures contained on DVDs. While computer hard drives capable of storing a DVD's content were rare in the consumer market of the early 90s, and home DVD burners were still a decade or so away, the eventual development of general purpose copy-capable equipment was a near certainty.[31] With this in mind, the studios developed the Content Scrambling System, or "CSS."

As described in the exceptional vocabulary section of Judge Kaplan's opinion in *Universal City Studios v. Reimerdes*,

CSS, or Content Scramble System, is an access control and copy prevention system for DVDs developed by the motion picture companies, including plaintiffs. It is an encryption-based system that requires the use of appropriately configured hardware such as a DVD player or a computer DVD drive to decrypt, unscramble and play back, but not copy, motion pictures on DVDs. The technology necessary to configure DVD players and drives to play CSS-protected DVDs has been licensed to hundreds of manufacturers in the United States and around the world.[32]

---

[29] "History of DVD", *at* http://www.absolute-playstation.com/api_faqs/ faq25.htm. The coding scheme they developed for video was MPEG-2. *See* Victor Lo, A BEGINNER'S GUIDE FOR MPEG-2 STANDARD, *at* http://www.fh-friedberg.de/ fachbereiche/e2/telekom-labor/zinke/mk/mpeg2beg/beginnzi.htm (last visited October 10, 2004). AC-3 was developed for surround-sound audio. *See* ATSC Standard, Digital Audio Compression (AC-3), Revision A, *available at* http://www.atsc.org/standards/a_52a.pdf (last visited October 10, 2004).

[30] "History of DVD," *supra* note 29.

[31] DVDs actually come in two "sizes." The "smaller" size, DVD-5, the size of most currently available blank DVDs, holds 4.438 GB of data, more than five times the data capacity of a CD. This is sufficient to store up to two hours of video encoded with the highest-quality MPEG-2 setting, but the capacity must also be shared by the audio tracks of the recording, making actual capacity somewhat less. The more common commercially produced DVD, DVD-9, nearly doubles the capacity of a DVD-5 by placing two layers of data inside the disc. The layer closer to the side that faces the reading laser in a player is semi-transparent, enabling a player or drive to "see through" the first layer when it reaches the end of the video stored there. *See* http://www.afterdawn.com/glossary/terms/dvd-9.cfm.

[32] Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 308 (S.D.N.Y. 2000). There are different combinations of CSS keys, corresponding to different licenses from the content industry, which differently enable players. The different licenses correspond to the ability to play only discs marketed for sale in certain geographical regions, to play multiple regionally-encoded discs, or, for the most elaborate and rarest licenses, to actually read the "1s" and "0s" as pure data, thus enabling a user to copy or modify the encoded data on the disc. *Id.* at

A DVD that is protected by CSS can only be accessed by a player or computer drive that conforms to a decryption algorithm, agreed to by the studios and electronics manufacturers, which employs a set of digital keys.[33] In other words, DVD players with the appropriate license keys allow a user to access the audiovisual or other software work encoded on a CSS-protected DVD, but not to read (and thereby copy) the pure binary data written on the disc. As such, CSS functions as both an "access control," because non-CSS enabled players cannot decode DVDs, and as a "copy control" because no consumer-grade DVD players manufactured under a studio license allow CSS-protected DVDs to transmit the data contained on a DVD to another medium for copying.[34].

The Internet and The Digital Dilemma

Even while tools to digitize and copy copyrighted works gained popularity in the early 1990s, a greater threat emerged – the internet. A world wide web of interconnected computers and ever-increasing transmission speeds meant that copies of works which in the analog world could only exist in their prime form in one location now could suddenly be in dozens, hundreds, thousands, or even millions of locations world wide at the touch of a button. Seemingly overnight, every digital pickpocket became a potential mob boss.[35]

---

n.63. Computer DVD drives run on driver software, which contains similarly licensed keys. DCC Report, *supra* note *20*, at 33.

[33] *Reimerdes*, 111 F. Supp. 2d at 310.

[34] As a postscript to this case study, it appears the studios were correct to bet on DVD. "As of 2000, about thirty-five percent of one studio's worldwide revenues from movie distribution was attributable to DVD sales and rentals." Universal City Studios, Inc. v. Corley, 273 F.3d 429, 437 n.3 (2d Cir. 2001). But the digital success story brought with it the risk of serious losses should the CSS keys become publicly available. As was the case with the Betamax, the MPAA saw this as evidence of a falling sky:

> Optical Disc Piracy is major threat to the audiovisual sector. Pirate optical discs, which include Laser Discs (LD), Video Compact Discs (VCD) and Digital Versatile Discs (DVD), are inexpensive to manufacture and easy to distribute. In 2000, over 20 million pirate optical discs were seized, and by comparison, 4.5 million videos were seized worldwide in the same period.

Motion Picture Association of America, *Anti-Piracy*, *available at* http://www.mpaa.org/anti-piracy (last visited October 10, 2004).

[35] The potential for widespread internet piracy became apparent when it was discovered that the successor to the MPEG-2 standard of compression used for DVD video could be used to compress digital music from CDs into very compact, high fidelity digital files. These "MP3" files were soon widely available on the internet, frequently without the authorization of the copyright holder in the musical work encoded therein. A&M Records v. Napster, Inc., 239 F.3d 1004, 1011 (9th Cir. 2001). The subsequent development of peer-to-peer software, which enabled users to "share" or "trade" MP3 files without the use of centralized servers as media storage made the digital pitfall that much greater. *Id.*

When in the mid-nineties a Norwegian hacker successfully cracked the CSS lock on DVDs with an application called "DeCSS," the potential threat of the internet to the growth of digital intellectual property crystallized:

> Once a decryption program like DeCSS is written, it quickly can be sent all over the world. Every recipient is capable not only of decrypting and perfectly copying plaintiffs' copyrighted DVDs, but also of retransmitting perfect copies of DeCSS and thus enabling every recipient to do the same. They likewise are capable of transmitting perfect copies of the decrypted DVD. The process potentially is exponential rather than linear.[36]

The National Academy of Sciences has referred to this situation as the "digital dilemma"[37] because digitized media, while offering the content industry unprecedented power to control, create, manipulate, package, and sell its wares, also has the "potential to demolish a careful balancing of public good and private interest that has emerged from the evolution of U.S. intellectual property law over the past 200 years."[38]

The threat from the internet has not fully matured. Presently, internet bandwidth limitations make the transmission of a decrypted DVD slow and unwieldy.[39] The content industry, however, has no intention of waiting for the information superhighway to turn into an autobahn traversed entirely by pirates. The Motion Picture Association of America (MPAA) has its own internet investigations unit[40] which has been monitoring developments to help produce forward-thinking

---

[36] *Reimerdes*, 111 F. Supp. 2d at 331.

[37] DCC Report, *supra* note 20, at 1.

[38] *Id.* at 3.

[39] It would take nearly 18 hours to transmit an hour of digital video with a comparable resolution to the analog VHS format over the typical high-speed cable or DSL internet connection. DCC Report, *supra* note 20, at 45. DVD-quality video, which has nearly double the video resolution of VHS, would take even longer to transmit with a typical connection. While DVDs that have been "ripped" (stripped of the CSS protection) can be efficiently compressed into smaller video files using the "DivX" compression standard (which enables the full-length feature to fit onto a single 650MB CD), this format alone requires between 10 and 20 hours of constant downloading to be completely reassembled on a new user's computer. *Reimerdes*, 111 F. Supp. 2d at 313-314. Moreover, the compression eliminates a great deal of the audio and video fidelity. *Id.* There is no guarantee that the source of the digital file will continue to make itself available during the entire process. Additionally, there is no guarantee that the user will receive what the file purports by its file name to contain, a piracy-thwarting technique employed with some success by the recording industry. "Oversight Hearing on Piracy on Peer-to-Peer Networks," (2002) *available at* http://www.riaa.com/news/newsletter/rosen_testimony092702.asp.

[40] *Reimerdes*, 111 F. Supp. 2d at 312.

strategies.[41] Fear of online piracy[42] has stifled the development of the full potential of the digital age.[43]

Finally, what makes matters worse with the internet is its lack of a central locus. The internet is simultaneously everywhere in the world. By acquiring access to foreign servers, an infringing distributor could more easily elude domestic prosecution. In the 1990s, this combined with another factor to increase the potential disaster for the content industry: globalization.

Globalization of American Media

Globalization in the 1990s changed the American media model from one in which domestic consumption was the only primary target (with foreign and ancillary markets being gravy), to a new model in which the foreign market was as important, if not more important to the bottom line.

Combined with an internet that, as noted above, may see domestic infringement largely enabled via websites located overseas, the globalization of American Media carried with it another dilemma – that opening up lucrative new markets provided foreign pirates a fertile ground of source material which could be distributed anywhere in the world, even to American users, without having to physically cross a border.

WIPO Treaty

While one solution to the digital dilemma was self-help – the content industry developed and continues to develop encryption and access

[41] By contrast, the computer software industry resigned itself long ago to the reality that upwards of 40% of users of business software are using illegally acquired copies. DCC Report, *supra* note 20, at 20-21.

[42] Once again, the MPAA is convinced the internet will spell the doom of its constituent members. "No one will pay for cable television or movies when they are available for free on the Internet." DCC Report, *supra* note 20, at 21.

> [However, the numbers indicate that, unlike "Napsterized" music,] movie box office receipts grew 13.5% in 2002—the best year-over-year performance in two decades. Growth in other media used for movie distribution was also dramatic. And revenues from videocassettes, the technology that was to have threatened the very security of the movie industry, exceeded box office receipts by $2 billion.

Id.

[43] S. REP. NO. 105-190, at 8 (1998) ("Due to the ease with which digital works can be copied and distributed worldwide virtually instantaneously, copyright owners will hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy."). Of course, not all digital content has shunned internet delivery. Perhaps the most obvious choice for internet distribution, computer software, has already adopted the internet as a popular distribution format. *See* DCC Report, *supra* note 20, at 14-16.

controls that protect its wares technologically[44] – it became clear that absent legal protection in markets both foreign and domestic, one of the most productive industries in history would lose ever-increasing percentages of potential revenues. With this understanding, the United States Government entered into the World Intellectual Property Organization (WIPO) Copyright treaty in the 1990s.

The most relevant articles of the treaty read as follows:

> Article 11
> Obligations concerning Technological Measures
> 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.
> ***
>
> Article 14
> Provisions on Enforcement of Rights
> (1) Contracting Parties undertake to adopt, in accordance with their legal systems, the measures necessary to ensure the application of this Treaty.
> (2) Contracting Parties shall ensure that enforcement procedures are available under their law so as to permit effective action against any act of infringement of rights covered by this Treaty, including expeditious remedies to prevent infringements and remedies which constitute a deterrent to further infringements.
> ***
>
> Article 22
> No Reservations to the Treaty
> No reservation to this Treaty shall be admitted.[45]

Both to comply with these new treaty requirements and to preemptively shield the increasingly technologically-based content industries, Congress enacted the Digital Millennium Copyright Act (DMCA) in 1998.[46] The centerpiece of the DMCA, the "WIPO Treaty Implementation Act," added to the Copyright Act, *inter alia*, 17 U.S.C. § 1201, which deals with anticircumvention protections for copyrighted works.[47]

---

[44] DCC Report, *supra* note 20, at 22.

[45] WIPO Copyright Treaty, Dec. 20, 1996, arts. 11, 14, 22, *available at* http://www.wipo.int/documents/en/diplconf/distrib/94dc.htm.

[46] Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C.).

[47] 17 U.S.C. § 1201 (2004). Arguably, the open nature of the language in Articles 11 and 14 of the WIPO treaty did not require any changes to Title 17. Before enactment of the DMCA, the grants of exclusive rights in 17 U.S.C. § 106 (2004), the enforcement mechanisms of Chapter 5, and the doctrines of contributory and vicarious infringement protected

The Current Version of § 1201

In one of the earliest cases decided under § 1201, *Universal City Studios v. Reimerdes*, Judge Kaplan gave an apt description of the statute's normative message:

> "[T]he strong right arm of equity" may be brought to bear against [those who would traffic in circumvention technologies or use them to violate copyright] absent a change in their conduct and thus contribute to a climate of appropriate respect for intellectual property rights in an age in which the excitement of ready access to untold quantities of information has blurred in some minds the fact that taking what is not yours and not freely offered to you is stealing.[48]

Congress constructed § 1201 as one of the most elaborate and complex sections in all of Title 17.[49] It consists of four basic components: 1) separate bans on three types of action; 2) a guideline for a rulemaking proceeding by which specific exemptions to the bans may be determined; 3) a series of congressionally-enacted exemptions; and 4) a detailed attempt to plug what has been termed the "analog hole."[50]

The Three Bans of § 1201

In the first two subsections of § 1201, Congress banned three types of activity (hereinafter "the bans"). These can best be described as the ban on hacking into an access control[51] (hereinafter "access hacking"); the ban on trafficking in technologies that foster or enable access hacking[52] (hereinafter "trafficking 1"); and a ban on trafficking in technolo-

---

all, or substantially all of the rights called for by the treaty in a manner that was "technology neutral." DAVID NIMMER, *A Riff on Fair Use in the Digital Millennium Copyright Act,* 148 U. PA. L. REV. 673, 683 (2000) [hereinafter NIMMER]. Further, because Article 11 of the WIPO Copyright Treaty bars acts "which are not authorized by the authors concerned or *permitted by law*," it would seem the rest of Title 17 would suffice. *See* WIPO Copyright Treaty, *supra* note 45 (emphasis added). However, the realization that the digital age presents new challenges, along with intense pressure from constituents like the MPAA, led to the passage of the statute. NIMMER, at 682 (citing Report of the Comm. on Commerce, H.R. REP. NO. 105-551, pt. 2, at 25 (1998)).

[48] Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 345 (S.D.N.Y. 2000).

[49] *See* Appendix A.

[50] DCC Report, *supra* note 20, at 28.

[51] 17 U.S.C. § 1201(a)(1) (2004) (providing that no person shall circumvent a technological measure that effectively controls access to a protected work).

[52] 17 U.S.C. § 1201(a)(2) (2004). This section provides that,

> (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

gies that foster or enable the circumvention of any technological measure that "effectively protects a right of a copyright owner under this title in a work or a portion thereof"[53] (hereinafter "trafficking 2").[54]

Access Hacking Ban

The first of the three bans is also the simplest, containing only three elements: 1) the existence of a work protected by copyright; 2) a technological lock barring unauthorized access to that work; and 3) circumvention of that lock.[55]

On its own, this ban is one of the most formidable provisions in copyright law which may be brought to bear on an individual for his own use of information. This is because the work protected by copyright need not be what the user is seeking to access when he bypasses the technological lock. It need only be contained within the same "fence" as the work or information the user is after to trigger this ban.

Trafficking 1

The first ban on trafficking in a technology[56] loosens the *Sony* standard for contributory infringement liability in the context of access hacking,[57] while supposedly leaving the *Sony* standard in place for in-

---

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

Id.

[53] 17 U.S.C. § 1201(b)(1) (2004). This section, "Additional violations," states that,

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

(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;

(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or 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.

Id.

[54] I prefer the terms "access hacking," "trafficking 1," and "trafficking 2" to "basic provision," "ban on trafficking," and "additional violations" because they are more descriptive and fit better into the reworked statutory language which I propose below. For a discussion on these terms, see NIMMER, *supra* note 48, at 684-685.

[55] 17 U.S.C. § 1201(a)(1).

[56] 17 U.S.C. § 1201(a)(2).

[57] "A given device or piece of technology might have 'a substantial noninfringing use, and hence be immune from attack under Sony's construction of the Copyright Act—but none-

fringement-enabling devices that do *not* involve hacking an access control mechanism.[58]

This broadens contributory infringement perhaps even more substantially than the access hacking ban broadens copyright infringement. Under the § 1201(a)(2) standard, a trafficker (which in the DMCA context includes manufacturers and software programmers)[59] is liable for producing a product with only "limited commercially significant purpose" beyond enabling a user to violate § 1201(a)(1)(A).[60] Now not only is the scope of use narrower, but the standard of liability is looser as well.

Acts which violate the trafficking 1 ban include the distribution of original software or hardware devices which grant access without a copyright holder's permission, such as DeCSS,[61] and distribution of tools that use the authorized access mode without the copyright holder's license or authority.[62]

---

theless still be subject to suppression under Section 1201.'" Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 323-24 (S.D.N.Y. 2000). "Indeed, Congress explicitly noted that Section 1201 does not incorporate Sony." *Id.* at 324.

[58] In contrast to the *Reimerdes* court's assertion, however, it is apparent that some in Congress felt they were passing a bill that fully incorporated the *Sony* standard, even in the context of circumvention.

> Given the language contained in the Judiciary Committee's original bill, specifically sections 1201(a)(1), (a)(2), and (b)(1), there was great reason to believe that one of the fundamental laws of copyright was about to be overruled. That law, known as *Sony Corporation of America v. Universal Studios*, 464 U.S. 417 (1978), reinforced the centuries-old concept of fair use. It also validated the legitimacy of products if capable of substantial non-infringing uses. The original version of the legislation threatened this standard, imposing liability on device manufacturers if the product is of limited commercial value. Now, I'm not a lawyer, but it seems irrational to me to change the standard without at least some modest showing that such a change is necessary. And, changing the standard, in a very real sense, threatens the very innovation and ingenuity that have been the hallmark of American products, both hardware and content-related. I'm very pleased that the conferees have meaningfully clarified that the Sony decision remains valid law. They have also successfully limited the interpretation of Sections 1201(a)(2) and (b)(1), the "device" provisions, to outlaw only those products having no legitimate purpose. As the conference report makes clear, these two sections now must be read to support, not stifle, staple articles of commerce, such as consumer electronics, telecommunications, and computer products used by businesses and consumers everyday, for perfectly legitimate purposes.

105 CONG. REC. H10621 (daily ed. Oct. 12, 1998) (statement of Rep. Klug).

[59] 321 Studios v. MGM Studios, Inc., 307 F.Supp.2d 1085, 1094-1095 (N.D. Cal., 2004).

[60] 17 U.S.C. § 1201(a)(2).

[61] *See Reimerdes*, 111 F. Supp. 2d at 294.

[62] 321 Studios v. MGM Studios, Inc., 307 F. Supp. 2d 1085, 1097-98 (N.D. Cal. 2004).

Trafficking 2

Trafficking 2 is somewhat less troubling than trafficking 1 ban because the devices it keeps out of users' hands are those which circumvent measures that "effectively protect a right of a copyright owner under this title in a work or portion thereof."[63] While this ban, like trafficking 1, lacks a specific intent element,[64] it at least shores up protections that were *designed* to protect rights which Title 17 already granted. Of the three bans, trafficking 2 is the most in line with the dictates of WIPO Treaty Article 11,[65] because its application is limited to the trafficking in technologies that allow circumvention of a device that "effectively protects a right of a copyright owner under this title in a work or portion thereof."[66] Clearly, however, there is some degree of overlap between trafficking 1 and trafficking 2. For example, public performance and display rights fall within those protected by trafficking 2, and yet, once access to a work is gained with a tool that violates trafficking 1, no other technological protection can prevent the user from violating those rights. Perhaps this overlap is why the cases have treated the tools banned in trafficking 2 as those which circumvent "copy" protections, [67] while those which are banned in trafficking 1 are treated as circumventing "access" protections.[68]

It is also interesting to note that, while trafficking 1 is mirrored by the user-side access hack ban, trafficking 2 has no parallel user-side ban. Two reasons for this have been given: 1) the rest of copyright law handles this issue;[69] and 2) Congress specifically did not want to foreclose the user from the possibility of circumventing a copy control to make fair use.[70]

CSS and The Three Bans

It is illustrative to evaluate how § 1201's three bans protect copyright holders who release films via CSS-encoded DVDs. Because CSS encoded DVDs require the device which plays the disc to have the

---

[63] 17 U.S.C. § 1201(b)(1) (2004).

[64] *See id.* ("For the purpose of violating an exclusive right of a copyright owner").

[65] DCC Report, *supra* note 20, at 22.

[66] 17 U.S.C. § 1201 (b)(1)(A)-(C).

[67] *See, e.g., 321 Studios*, 307 F. Supp. 2d at 1095, 1097.

[68] Universal Studios Inc. v. Corley, 273 F.3d 429, 452 (2d Cir. 2001). Note that both DeCSS, enjoined in *Corley* for circumventing the access protection, and DVD X Copy, enjoined in *321 Studios* for circumventing a copy protection, are software applications that *specifically* circumvent the same program - CSS.

[69] NIMMER, *supra* note 48, at 691.

[70] *321 Studios*, 307 F. Supp. 2d. at 1097; *see also* United States v. Elcom, Ltd., 203 F. Supp. 2d 1111, 1120 (N.D. Cal. 2002). For a counter-argument to this position, see *infra* Part II.C.

compliant license keys, § 1201(a) clearly applies. However, in order for a user to violate the access hack ban, he would somehow have to find a DVD drive with a laser and optical reader capable of reading the 1s and 0s on the DVD but nevertheless manufactured and sold without licensing the CSS keys.[71] This task would be more cumbersome than effectuating the access hack. What makes this so absurd is that there is no reason for manufacturers to produce drives without the CSS keys and no market for their purchase. At least insofar as the access hack ban is concerned, the mere fact of CSS does the trick, absent any need for legal protection. Similarly, there is little commercial value in producing a DVD drive which has not licensed the CSS keys from the studios. Hence, trafficking 1 bars the distribution of a device that is so useless that no real threat exists.

The same cannot be said for trafficking 2. Because virtually every DVD-playing drive on the market already has access to the work protected by the § 1201(a) aspects of CSS, what the would-be hacker desires is a means to circumvent the *copy* controls, i.e., to be able to read the 1s and 0s, not as video and audio, but as 1s and 0s, thus enabling duplication and modification of that data. Trafficking 2 therefore is a legal restriction with teeth.

The Protections For Users

Copyright law has always maintained the "delicate balance"[72] called for by the intellectual property clause of the constitution, i.e., to secure exclusive rights to writers and inventors in their creations so as "to promote progress in science and the useful arts."[73] In enacting § 1201, Congress made sure that some measures were incorporated to maintain some semblance of this balance.

The first of these measures involves what does *not* appear in § 1201 – the user-side ban in subsection (b).[74] Because some form of circumvention may be necessary to engage in fair uses of the copyrighted work, this section does not appear.

---

[71] For example, the mythical LINUX DVD drive referred to frequently in *Reimerdes* 111 F.Supp.2d at 311. Somehow, *Reimerdes* nevertheless found the defendants liable under "trafficking 1." *See infra* Part II.

[72] NIMMER, *supra* note 48, at 74.

[73] U.S. CONST. art. I, § 8.

[74] *See infra* Part II.F.

The Savings Clause

Further, subsection (c), entitled "other rights, etc., not affected,"[75] contains two protections for users. The most pointed of these says, "Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title."[76] While on its surface this appears to give users some wiggle room with respect to the three bans, the cases have consistently said otherwise.[77] While Congress apparently inserted § 1201(c)(1) for fear that §§ 1201(a) and (b) would deny users the "bread" of fair use and a public domain, it also appears the response of the courts has been to say "so let them eat cake."[78]

The Rulemaking Proceeding

In recognition of the possibility that users who cannot hack an access control may be denied fair use rights in ways not foreseeable when the statute was enacted in 1998, Congress inserted an elaborate

---

[75] 17 U.S.C. § 1201(c) (2004).

[76] 17 U.S.C. § 1201(c)(1) (2004).

[77] [Defendants] contend that subsection 1201(c)(1), which provides that 'nothing in this section shall affect rights, remedies, limitations or defenses to copyright infringement, including fair use, under this title' can be read to allow the circumvention of encryption technology protecting copyrighted material when the material will be put to 'fair uses' exempt from copyright liability . . . . [§ 1201(c)(1)] simply clarifies that the DMCA targets the circumvention of digital walls guarding copyrighted material (and trafficking in circumvention tools), but does not concern itself with the use of those materials after circumvention has occurred. Subsection 1201(c)(1) ensures that the DMCA is not read to prohibit the 'fair use' of information just because that information was obtained in a manner made illegal by the DMCA.

Universal City Studios, Inc. v. Corley, 273 F.3d 429, 443 (2d Cir. 2001); *see also* 321 Studios v. MGM Studios, Inc., 307 F. Supp. 2d 1085, 1102 (N.D. Cal. 2004) ("Again, however, while purchasers of DVDs with material in the public domain unquestionably have the right to make use of this public domain material, they can simply access it from a non-CSS encrypted DVD or can choose to access and copy this public domain material in a non-digital form.").

> While the DMCA may make certain fair uses more difficult for digital works of authorship published with use restrictions, fair use has not been eliminated. Similarly, the argument that Congress' ban on the sale of circumvention tools has the effect of allowing publishers to claim copyright-like protection in public domain works is tenuous and unpersuasive. Nothing within the DMCA grants any rights to anyone in any public domain work. A public domain work remains in the public domain and any person may make use of the public domain work for any purpose.

United States v. Elcom Ltd., 203 F. Supp. 2d 1111, 1141 (N.D. Cal. 2002).

[78] The other § 1201(c) protection for users is found in paragraph (4), which provides that, "Nothing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products." 17 U.S.C. § 1201(c)(4) (2004). This provision merely asks courts not to allow § 1201 to exceed the limitations of the First Amendment - i.e., it prevents the government from applying the law in a way that amounts to an unconstitutional ban on free speech. *See* U.S. CONST. amend. I ("Congress shall make no law . . . abridging the freedom of speech.").

rulemaking proceeding in which "the Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation,"[79] shall every three years come up with a list of classes of works, the fair use of which has been adversely affected by the access hacking ban.[80] The users of classes of works contained in this list are exempt from liability under § 1201(a)(1)(A) during the succeeding three year period.[81]

User protections afforded by this rulemaking are limited. First, because the exemptions apply only when users are deemed to be "of a particular class of copyrighted works,"[82] this prevents the enactment of blanket exemptions which would apply equally to all digitally-encoded copyrighted works.[83] If the beast Congress created in § 1201 has swallowed all of copyright law, this rulemaking proceeding will provide no relief from the access hack ban. Further, even where exemptions are granted, they only remain in effect for the subsequent three years.[84]

Second, subparagraph (E) makes explicit that the exemptions promulgated do not apply to either of the trafficking bans.[85] This produces the recurring paradoxical situation in which a user, though "free" to hack through an access control, will be unable to do so with any tools he cannot engineer on his own.[86]

A third, more pragmatic limitation has evolved in the two rulemaking proceedings which have already taken place. This is discussed at length in Part II.E., *infra.*, but for now, it should suffice to say that the process has been a miasma of bureaucracy, featuring interagency squabbling about burdens of proof, the definition of "particular class of copyrighted work," and the nature of evidence required.[87]

The Statutory Exemptions

Finally, Congress enacted a series of exemptions for nonprofit libraries, archives, and educational institutions;[88] law enforcement, intel-

[79] 17 U.S.C. § 1201(a)(1)(C) (2004).
[80] *Id.*
[81] 17 U.S.C. §§ 1201(a)(1)(B)-(D) (2004).
[82] 17 U.S.C. § 1201(a)(1)(C).
[83] NIMMER, *supra* note 48, at 694-695. *See also infra* Part II.C.
[84] NIMMER, *supra* note 48, at 696.
[85] 17 U.S.C. § 1201(a)(1)(E) (2004).
[86] NIMMER, *supra* note 48, at 736-737.
[87] *See infra* Part II.E.
[88] 17 U.S.C. § 1201(d) (2004).

ligence, and other government activities;[89] reverse engineering;[90] encryption research;[91] prevention of access to materials on the internet to minors;[92] protection of personally identifying information;[93] and security testing.[94] The details of these exemptions are not what matters: what does matter is that the various exemptions do not all apply to the same subset of the three bans.[95]

Plugging the Analog Hole

One loophole in the digital revolution is what has been called the "analog hole."[96] This backdoor through technological measures like CSS exists when the audio or video feed, having already been decoded into perceivable analog form by passing through an authorized player, is redigitized into a near-perfect copy which lacks the original technological protections.[97]

Several technologies have been developed to try to plug the analog hole. The most successful of these, the gain control or "macrovision" standard for analog video recorders, is enshrined in the last and longest subsection of § 1201. [98] This subsection requires all analog video recording devices to comply with the standard.[99]

---

[89] 17 U.S.C. § 1201(e) (2004).

[90] 17 U.S.C. § 1201(f) (2004).

[91] 17 U.S.C. § 1201(g) (2004).

[92] 17 U.S.C. § 1201(h) (2004).

[93] 17 U.S.C. § 1201(i) (2004).

[94] 17 U.S.C. § 1201(j) (2004).

[95] NIMMER, *supra* note 48, at 700-701.

[96] DCC Report, *supra* note 20, at 28.

[97] *Id.*

[98] 17 U.S.C. § 1201(k) (2004).

[99] *Id.* Some observations are in order. First, it appears as though § 1201(k) is in direct conflict with the "no mandate" clause, 17 U.S.C. § 1201(c)(3) (2004). Because the legislative history indicates that subsection (k) was added late in the game, this conflict may have gone unnoticed. H.R. REP. NO. 105-551.

Second, the macrovision requirement has largely gone unheeded. Having purchased two VHS recorders since the enactment of § 1201, one manufactured by Sharp, the other by Sony, I can personally attest to the fact that DVD players whose signals have passed through both VCRs en route to my television displays have never shown any degradation from the supposed macrovision requirement, despite well over 100 unique DVD titles being played through this "analog hole." (N.B. Since the Betamax case in the 70s, while Sony has reluctantly moved to the VHS standard for analog video recording, it has also purchased Columbia Tristar studios, and, more recently, MGM. *See* http://www.darkhorizons.com/news04/040914a.php. Thus, Sony is in the unique position of wearing the hats of a constituent member of the MPAA and a consumer electronics manufacturer, which seemingly puts Sony at odds with itself in every § 1201 debate). *See* "Sony, the Conflicted Conglomerate," (2002) *available at* http://news.com.com/Sony+The(c)onflicted(c)onglomerate/2009-1040_3-936522.html.

PART II: A PROPOSAL EDUCATED BY HINDSIGHT

With the advantage of six years of hindsight, several high-profile court decisions, a series of studies, and some amendments proposed by members of Congress, the time is ripe for the long, unwieldy, and faulty § 1201 to be reworked as a more perfect statute. [100]

To begin, even the MPAA's post-Napster fears of digital Armageddon appear to be overblown. New business plans always emerge to accommodate not just changes in law, but changes in the "real" world.[101]

A. *Overview of Changes*

The cardinal rule of new legislation is to design it so that it does no harm as it takes action on whatever condition required its passing.[102] Perhaps because § 1201 was passed at a time when the nascent digital industry had yet to mature, its current incarnation fails in this respect. As the DCC report notes, "we should be careful not to unnecessarily perpetuate rules that were created for a world made up of atoms that were physically distributed."[103]

With that in mind, I propose that § 1201 be amended to conform to Appendix B of this paper. The principal changes are as follows.

First, given its unwieldy nature, § 1201 has been divided into two statutes. My proposed § 1201 contains the enumeration of banned activities, the analog macrovision requirements, the subsection (c) savings clauses, and a new subsection (d), described in Part II.B., *infra*. The administrative procedures and exemptions have been relocated to my proposed § 1201A, along with a new "digital fair use" defense.

Second, §§ 1201(a) and (b) have been modified to better parallel each other. The first such modification was to rename (b) from the monumentally unhelpful "additional violations" to a far more descrip-

---

Finally, the MPAA continues to develop a watermarking technology that will survive the digital-analog-digital process. DCC Report, *supra* note 20, at 28-29. While the feasibility of this technology will enable investigators to more easily track down access hack violators, it appears unlikely this standard will become universally adopted without accompanying legislation or regulation, which would run afoul of § 1201(c)(3).

[100] The House of Representatives apparently echoes this sentiment. Robert Moore, the president and founder of 321 Studios (the party in the DVD X Copy litigation) was called to testify on May 12, 2004 at a hearing on the Digital Media Consumers' Rights Act of 2002, H.R. 5544, 107th Cong. (2002), *available at* http://www.techlawjournal.com/cong107/copyright/boucher/20021003bill.asp.

[101] "Thus, as the content industry is finding, there are ways to compete with 'free'—as the ever-increasing number of people carrying around bottles of purchased spring water demonstrate." DCC Report, *supra* note 20, at 48.

[102] *Id.* at 46.

[103] *Id.*

tive "copyright control circumvention violations." Also, my proposed subsection (b) has both a trafficking and user-circumvention ban, which should afford additional protection to copyright holders. Further, to clean up the miasma of what type of control measure is being employed in a particular situation, the definitions of "access control" and "copyright control" have been refined. These revised definitions at least partially return § 1201 to the technologically neutral version of copyright law, because they focus more on why the technological measure is circumvented than on what it was designed to protect.

Third, to answer the much-articulated fears that allowing content producers to build electronic or digital fences around content that is in the public domain or otherwise not theirs to control, my proposed subsection 1201(d) defines a complete affirmative defense entitled "anticircumvention misuse," discussed in Part II.B., *infra*.

As a fourth major change, discussed at length in Part II.E., *infra*, the Librarian of Congress' triennial reports concerning effects of applications of the § 1201 bans have a reduced regulatory impact. Rather than serving as regulations promulgated pursuant to a Congressional delegation of authority and carrying the force of law, these findings now have two meanings. First, they stand as recommendations for Congressional enactment as new exemptions to some or all of the bans of §§ 1201(a) and 1201(b). And second, they serve as a factor in the balancing test established for the new digital fair use defense.

Not surprisingly, the fifth major change is found in my proposed § 1201A(e), entitled "digital fair use." This subsection, which borrows extensively from bills proposed by United States Representatives Boucher[104] and Lofgren,[105] is the major focus of Part II.C., *infra*. In a nutshell, my proposed § 1201A(e) creates exemptions for both users who circumvent access and copyright controls, and alleged traffickers in technologies which enable fair circumvention by users.

Finally, my proposed § 1201A(d) serves as a repository for all previously enacted exemptions to the various § 1201 bans. It also incorporates several exemptions based on the two rounds of rulemaking conducted by the Librarian of Congress.

---

[104] Digital Media Consumers' Rights Act of 2002, H.R. 5544, 107th Cong. (2002).

[105] Benefit Authors without Limiting Advancement or Net Consumer Expectations (BALANCE) Act of 2003, H.R. 1066, 108th Cong. (2003), *available at* http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.1066:.

B. *Let Copyright Be Copyright*

The day before the DMCA was enacted, Congress passed the Sonny Bono Copyright Act, which not only "superincentivized" the creation of new works by extending copyright terms an additional twenty years, but also somehow managed to reincentivize extant works by giving them the same extension.[106] Coupled with the DMCA, it was suddenly apparent that Title 17 had begun to eat away at the public domain which the Constitution mandates be left outside its ambit. Section 1201 added to this in two ways, which my current proposal attempts to address.

The first of these is the creation of new rights not previously enjoyed under copyright law. Traditionally, the principal rights of copyright holders were in reproduction, preparation of derivative works, distribution of copies and phonorecords, public performance, public display, and the sui generis digital audio transmission right.[107] Suddenly, with § 1201(a), a right to control access to a work existed.[108] This access control runs the danger of protecting works that are not protected by copyright.[109]

This possibility exists for two reasons: 1) when even the lengthy Sonny Bono Act copyright term in a work expires, works produced today may exist only in copies that are protected by access controls which will most likely still be in place when that term expires;[110] and 2) the

---

[106] Sonny Bono Copyright Term Extension Act, Pub. L. No. 105-298, 112 Stat. 2827 (1998).

[107] 17 U.S.C. § 106 (2004).

[108] Admittedly, an access control right may be a necessary addition in the digital world. Because unauthorized copies of digitally encoded works are perfectly identical clones of the original, the § 106 reproduction right does little in physical terms to protect the copyright holder without the ability to control *access* to a copy once it is produced. Similarly, because the distribution right can, thanks to the internet, be exercised in fact *before* the reproduction right (the very nature of digital, on-line distribution), the copyright holder can do little to block unauthorized distribution of his work. Hence, an access control right returns a great deal of this control to its rightful owner.

[109] DCC Report, *supra* note 20, at 40-41.

[110] Nimmer, *supra* note 48, at 693. There are two counters to this argument: First, technological measures may be designed so as to stop functioning upon the expiration of copyright. Given the various ways copyright terms may terminate and the uncertainty of future Congressional action, however, it would be difficult to conceive of an access or copy control system that can accommodate all possible eventualities. The other argument was issued in the opinion in *Elcom*:

> A public domain work remains in the public domain. Any person may use the public domain work for any purpose - quoting, republishing, critiquing, comparing, or even making and selling copies. Publishing the public domain work in an electronic format with technologically imposed restrictions on how that particular copy of the work may be used does not give the publisher any legally enforceable right to the expressive work, even if it allows the publisher to control that particular copy.

possibility exists that an access or copy control may be erected around a storage medium which contains both works to which the producer has exclusive rights, and some to which he never enjoyed such rights. This "bundling" effect allows an amount of capture that cannot be protected by copyright, either because they lack originality, because they are not covered under the § 102 list of categories of protected works, or because they have lapsed into the public domain.[111]

My proposed § 1201(d) attempts to ensure that § 1201 did not needlessly expand copyright to incorporate these scenarios.[112] It reads:

> (d) Anticircumvention misuse.
>
> (1) The bundling of works which reside in the public domain, or which are otherwise not protected by this title, and which are not reasonably available in another form by potential users of those works, within an access control subject to subsection (a) of this section, shall constitute "anticirumvention misuse," and shall bar a plaintiff from bringing any action under this section.
>
> (2) Works shall be deemed "reasonably available in another form" within the meaning of paragraph (1) if the producer or marketer of the work which would otherwise fall within the bar of paragraph (1) includes a method of accessing the unprotected works in a user interface which is readily accessible by any potential user.
>
> (3) Anticircumvention misuse as defined in this subsection shall not serve as a defense to the infringement of any other right protected by this title.

This proposed section distinguishes between access controls and copyright controls in the context of anticircumvention misuse. Also, paragraph (2) addresses the concern that the anticircumvention misuse defense as construed might delve into the realm of antitrust, and also better warns media producers of what they can do to avoid losing the § 1201(a) and (b) protections.

United States v. Elcom, Ltd., 203 F. Supp. 2d 1111, 1134 (N.D. Cal. 2002). The short-sightedness of this argument has already been discussed, however: should *all* copies of the public domain work be locked away behind such controls, the work can no longer be said to be "in the public domain" for practical, if not legal, reasons. The *Corley* court rejected the logic of this argument on two separate grounds: 1) that it was argued in a footnote of a brief, so was not to be considered part of the argument before the court; and 2) because the problem had not yet matured and hence remained speculative. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 445 (2d Cir. 2001). Query whether *informed* speculation should void proposed legislation under the "do no harm" theory.

[111] *See* Howard Besser, "Copyright Dangers and the Importance of Fair Use" (2002), *available at* http://www.gseis.ucla.edu/~howard/Copyright/Elect-publ00/ ppframe.htm.

[112] I am indebted to my fellow Advanced Copyright Seminar scholars who debated the earlier version of this proposal in a mock Congressional Committee, chaired by no less a copyright expert than "Congressman" David Nimmer on March 1, 2004. Their feedback largely informs this final proposal.

A hypothetical example may be helpful: Assume that Producer "P" has put together a multimedia CD-ROM of the complete works of Shakespeare, complete with original illustrations and *interpretive* notes. These illustrations and notes would certainly be entitled to copyright protection, which would allow P to place an access control mechanism that bars unauthorized users from accessing his CD-ROM. The Complete Works of Shakespeare, on the other hand, most certainly reside within the public domain.

Now assume that virtually all known copies of Shakespeare's writings have, by the time of P's CD-ROM release party, ceased to exist. Under the plain meaning of the language in paragraph (1), those works are not reasonably available in another form to potential users.

So what is P to do? Section 1201 gives him the legally enforceable right to protect his original materials within an access control measure, but under § 1201(d)(1), P does *not* have the right to similarly tie up the Shakespeare texts. The solution is presented in my proposed § 1201(d)(2): P need merely create a separate directory for the text-only elements which inhabit the public domain and which can be accessed without having to go through an access control measure.[113] By following this suggestion, P is not guilty of "misuse," and he can enjoy the protections of § 1201(a).

Similar para-copyright problems became most apparent in two recent cases in which § 1201 was invoked, perhaps allowing dangerously anticompetitive results.[114] In *Lexmark v. Static Control*,[115] computer printing giant Lexmark "successfully alleged that Static Control's microchip 'spoofed' its copyrighted software in violation of the DMCA" by copying Lexmark's automatic subroutine onto its own after-market toner cartridge microchips.[116] Because this unauthorized spoofed software initialized the "it's okay to print" security measure built into the printer by Lexmark (enabling it to function as though a Lexmark cartridge were in place), and because computer software is considered to be protected by copyright, this was considered an access

[113] If P is concerned this will negatively impact his artistic presentation within the protected expression, he can simply program the access-control-blocked software to perform the transformations on the text, which it, too, reads from the text file.

[114] DCC Report, *supra* note 20, at 32.

[115] Lexmark Int'l, Inc. v. Static Control Components, Inc., 253 F. Supp. 2d 943 (E.D. Ky. 2003).

[116] DCC Report, *supra* note 20, at 32. The report notes in a footnote that "During a recent Copyright Office hearing concerning additions to DMCA exemptions, Former Register Ralph Oman, representing Lexmark, at one point appeared to assert that users need permission to run a computer program, and consequently that if users use a computer program for a purpose of which its author disapproves, they are infringers." *Id.*

hack violation. However, the DMCA issue was completely sidestepped in the similar case of *Chamberlain v. Skylink*,[117] because the garage door opener manufacturer did not give notice that its software-encoded mechanism was not permitted to interoperate with outside manufacturers' replacement remotes.[118]

To address these *Lexmark* and *Chamberlain* type issues, the distinctions between "access controls" and "copyright controls" must be refined. Because the concern in cases like *Lexmark* is that copyright law appears to be reaching subject matter it was never meant to reach, it seemed apparent that these cases hung their shingles under the ambit of access, and not copyright control. Hence, my proposed § 1201(a)(3)(B) reads:

> (3) As used in this subsection—
>
> (B) "access" means the ability to perceive a writing, audiovisual work, performance or phonogram, or to manually execute a computer software application . . . .

This language solves the *Lexmark* problem by limiting the access controls that protect software applications to such software as is actually "manually executed" by the user. Because the access control is not a *copyright* control (that is covered by § 1201(b)), the statute can be more limited in its approach to software as a "work protected under this title." The access control protections will be available to producers and distributors of all kinds of digital media, while no longer giving an anticompetitive edge to the crafty hardware manufacturer who sneaks "copyrightable expression" into his products in ways no reasonable user would ever appreciate.

C. *Saving Fair Use*

In total, my proposed §§ 1201(a)(3)(B) and 1201(d) should help prevent the "pay-per-use" society feared by commentators,[119] policymakers,[120] and legislators.[121] To further protect against this eventuality, it is necessary to defend copyright law from some potential attacks on

---

[117] Chamberlain Group, Inc. v. Skylink Techs., Inc., 292 F. Supp. 2d 1040 (N.D. Ill. 2003) (Aff'd by Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178 (2004)).

[118] *Id.* at 1042.

[119] *See* NIMMER, *supra* note 48.

[120] *See* DCC Report, *supra* note 20.

[121] *See supra* notes 105 and 106 and accompanying text.

the fair use doctrine enshrined in § 1201[122] and the cases decided under it.[123]

It has been noted that passage of the WIPO Treaties Act did not necessitate any changes to the Fair Use provisions of § 107 because Fair Use has always been "technologically neutral."[124] Yet the upshot of § 1201 is that access to a work must be lawfully acquired before a use can be fair.[125] In a truly "technologically neutral" world, the pre-digital disregard for how access was achieved[126] in the fair use inquiry would translate into the post-digital DMCA world, as well. However, it is necessary to modify § 1201 to create a "digital fair use" defense to the process of gaining access to copyright-protected materials to allow one to make traditional fair use of the works themselves.

The cases have grappled with the fair use problem. Although *Corley* and *Elcom* dismissed the notion that fair use is a constitutional mandate, the Supreme Court rejected that view in *Eldred v. Ashcroft*:

> [C]opyright law contains built-in First Amendment accommodations. First, it distinguishes between ideas and expression and makes only the latter eligible for copyright protection . . . . Second, the "fair use" defense allows the public to use not only facts and ideas contained in a copyrighted work, but also expression itself in certain circumstances.[127]

However, in the wake of *Eldred*, the *321 Studios* case held specifically that "§ 1201 does not eliminate fair use, and the doctrine of fair use does not guarantee copying by the optimum method or in the identical format of the original."[128] The Court elaborated:

> Fair use is still possible under the DMCA, although such copying will not be as easy, as exact, or as digitally manipulable as plaintiff desires. Furthermore, as both Corley and 321 itself stated, users can

---

[122] With due deference to *Corley*, *see supra* note 111; while these dangers remain speculative at this point, it is worth noting that the only other protection would be to ensure a vibrant analog world. However, both audio and video productions are steadily moving towards an all-digital environment, and while there continues to be a vibrant publishing industry for printed materials, already this researcher has managed to write this entire proposal using only sources found online, in digital formats.

[123] For example, Judge Kaplan in *Reimerdes* acknowledged the possibility that 17 U.S.C. § 1201 may have unduly upset the balance of fair use protections, but decided that the erosion of fair use did not absolve the defendants for their § 1201 violations. Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 304 (S.D.N.Y. 2000).

[124] NIMMER, *supra* note 48, at 723.

[125] *See* 321 Studios v. MGM Studios, Inc., 307 F. Supp. 2d 1085, 1097-98 (N.D. Cal. 2004) ("This Court finds, as did both the *Corley* and *Elcom* courts, 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).").

[126] *See* Harper & Row, Publishers, Inc., v. Nation Enters., 471 U.S. 539 (1985).

[127] Eldred v. Ashcroft, 537 U.S. 186, 219 (2003) (citation omitted).

[128] *321 Studios*, 307 F. Supp. 2d at 1104.

> copy DVDs, including any of the material on them that is unavailable elsewhere, by non-digital means. 321's assertion that this would impermissibly place a financial burden on users' First Amendment rights is both an overstatement of the extent of the fair use doctrine and a misstatement of First Amendment law. A financial burden would only render a statute unconstitutional if it was placed on the speaker because of the content of the speech, not because of the speaker's desire to make such speech.[129]

However, this does not fully address the issue. As noted in Part I, *supra*, § 1201(k) largely closes the "analog hole" (at least in theory), thus making the "legal" fair use contemplated in *321 Studios* more difficult to imagine. In other words, in many foreseeable situations, the would-be fair user now has a right to engage in one set of activities that are nevertheless made impossible by restrictions placed on activities which must necessarily precede those that are legal.[130]

The Congressional response has been that this is why § 1201(b) contains no user-side ban (i.e. because fair use is a defense to copyright infringement, the individual user should be able to circumvent copyright protections so as to make fair use).[131] But trafficking 2 prevents a would-be fair user from acquiring the tools necessary to do so.[132] This is akin to a statute that, in subsection (a) grants all individuals the right to fly, but in subsection (b) bans the trafficking in or commercial exploitation of aircraft, helicopters, gliders, jetpacks, and all other technological flight-enabling implements.[133]

---

[129] *Id.* at 1102 (citations omitted).

[130] *See* NIMMER, *supra* note 48, at 729 n.302.

[131] *Id.* at 716 n.237.

[132] *See* "TESTIMONY OF ELECTRONIC FRONTIER FOUNDATION (EFF) BEFORE COPYRIGHT OFFICE PUBLIC HEARINGS ON DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA)," (2002) *available at* http://www.virtualrecordings.com/EFFtestimony.htm.

[133] The best-articulated argument on this point that I have seen is found in the DCC Report:

> It is one thing for society to make some action "wrong" or "illegal." It is quite another for society to enable private parties to make an otherwise lawful action impossible. Building digital walls may be antithetical to building trust and that sense of community that is essential to encouraging voluntary compliance with law—particularly if those walls do not reflect shared values. Building such walls is the technological equivalent of Prohibition—and will likely be as successful. If our government tells us that we may only use systems that obey the "authorization" mandates of others, and those mandates ignore shared values, many among us may seek to breach the walls in order to act in ways that we have been accustomed to doing, and which the law has previously authorized. If we substitute electronic fences for internalized values, and technical controls for publicly created law, we may lose our collective moral bearings and the considerable benefits of self-enforcement.

DCC Report, *supra* note 20, at 41.

My proposed § 1201A(e)[136] attempts to rescue fair use from this web of impracticability:

(e) Digital Fair Use
  (1) It is not a violation of sections 1201(a)(1) or 1201(b)(1) to circumvent a technological measure in connection with access to, or the use of, a work if such circumvention does not result in an infringement of the copyright in the work.
  (2) Fair Trafficking
    (A) The manufacture, distribution, importation or marketing of a hardware or software product that is reasonably necessary to circumvent an access or copyright protection control as allowed under subsections (d) or (e)(1) shall be considered fair trafficking if that hardware or software product is capable of substantial noninfringing use, and shall not violate sections 1201(a)(1) or 1201(b)(2).
    (B) In determining whether or not an act of trafficking is fair within the meaning of paragraph (A), a court shall consider:
      (i) the failure, if any, of the copyright holder to make publicly available the necessary means to perform noninfringing uses as described in paragraph (1) without additional cost or burden to the user of the work;
      (ii) the extent to which the design and marketing of the product or device challenged under section 1201(a)(2) or 1201(b)(2) is limited to enabling noninfringing uses;
      (iii) the reasonableness of the consumer expectations for noninfringing uses which could not be met absent such a product or device;
      (iv) the availability and suitability of alternative works or versions of works to the noninfringing uses most likely to be desired by the intended customers of the product or device;
      (v) the inclusion or exclusion of the circumvention means or class of works most affected by it in the reports of the Librarian of Congress published under subsection (c); and
      (vi) such other factors as the court considers relevant to determining the fairness of barring the trafficking of the specific product.

Paragraph (1) of this section does away with the clear and convincing standard, which had been included as a compromise to allay fears that giving a traditional fair use defense to the two trafficking bans would destroy the protections of § 1201. Traditional copyright defenses

would *only* apply to the user-side bans of my proposed §§ 1201(a)(1) and 1201(b)(1).[134]

The second paragraph, which defines a "fair trafficking defense," is patterned on the balancing test of § 107.[135] There are several rationales for this balancing test. First, it gives factors which encourage potential plaintiffs to avoid applying digital locks that protect rights which the rest of Title 17 does not actually grant copyright holders. Second, it gives meaning to the scaled-back administrative proceeding discussed in Part II.E., *infra*. Third, the inclusion in subparagraph (A) of the language, "substantial noninfringing use," aligns the trafficking bans with the *Sony* standard which was disclaimed by § 1201, but which remains in line with longstanding consumer expectations.

The DCC report, which supports the proposal that the digital fair use defense is necessary, states:

> The problem with the content industry argument [that greater certainty with DRM will enable the offering of more user choices] is that the ability to offer many choices carries with it the ability to offer only one choice. In the end, users are left with the content industry's promise that they will have choices—or with the argument that in a world in which distribution is cheap and perfect price discrimination is possible, everyone will be able to obtain what they are willing to pay for. But if the content industry chooses to offer only one profit-maximizing option—say, pay-per-view—for all of its cultural artifacts, and if the law provides no alternative path for access (even for the purposes for which fair use was codified), users will find the sphere of publicly available material shrinking rapidly.[136]

Under the new digital fair use standard, the *321 Studios* case would have had a different outcome. The product at issue in that case, DVD X Copy, would likely prevail on the balancing test. Following the longstanding belief that users have fair use rights in making back-up copies of digital works they have acquired legally,[137] the ability to make back-up copies of one's DVD library should be protected as fair use.[138] As such, DVD X Copy has a "substantial noninfringing use." But unless the user has the programming skills of Jon Johansen (the creator of DeCSS),[139] he cannot exercise this right without some form of "traf-

---

[134] *See infra* Part II.F.

[135] 17 U.S.C. § 107 (2005).

[136] DCC Report, *supra* note 20, at 41.

[137] TESTIMONY OF ELECTRONIC FRONTIER FOUNDATION (EFF) BEFORE COPYRIGHT OFFICE PUBLIC HEARINGS ON DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA), *supra n.* 132.

[138] As anecdotal evidence of the necessity for backups, my apartment was burglarized two years ago, and all that the thief stole was $500 worth of DVDs.

[139] *Reimerdes, supra* note 32.

ficked" technology. In other words, the user has a right which is impossible for him to exercise.

Further, DVD X Copy contains several protections that prevent it from easily being used for widespread piracy. First, every DVD produced with the software, when played, displays a warning screen which tells the user the legal limits of his fair use rights.[140] Second, unlike other software applications which create hard copies of digital works (like the "print" command of a word processor), DVD X Copy has no "make multiple copies" option, meaning the backup process must be repeated for every copy the user wishes to make.[141] Similarly, the software only writes to one DVD burner per backup, thus preventing the writing of copied DVDs *en masse*. Finally, the software deletes the decoded DVD data as soon as the backup process is complete, thus preventing the user from burning multiple copies of the backed-up data without having to first re-decrypt the original.

D. *Freeing the Innovators and Technophiles*

One fear that the *321 Studios* case produced was that such applications of § 1201 would stifle the creation of technologies that meet legitimate consumer expectations, yet potentially run afoul of a strict reading of the statute.[142]

Another fear that has been articulated is that, because the intellectual property clause of the constitution specifies that intellectual property protection is meant to "further the progress of science and the useful arts," § 1201 may prevent the contemplated stepping on the shoulders of giants.[143] This undercuts the possibility of revolutions in technology or business models.[144]

Finally, the digital fair use provisions included above address some of the concerns that research efforts, while seemingly exempted from prosecution under §§ 1201(f) and 1201(g), were nonetheless being de-

---

[140] The warning screen reads:

> You are viewing an archival backup copy of a DVD, created solely for the private and personal use of the owner of the DVD from which it was made. Federal copyright laws prohibit the unauthorized reproduction, distribution, or exhibition of copyrighted materials, if any, contained in this archival backup copy. The resale, reproduction, distribution, or commercial exploitation of this archival backup copy is strictly forbidden. We ask you to respect the rights of copyright holders.

(On file with author).

[141] With currently available technology, this process takes roughly one hour per DVD.

[142] *See* DCC Report, *supra* note 20, at 38-39.

[143] *Id.* at 8-9.

[144] *Id.* at 31.

terred by the restrictions in place under the statute and existing Digital Rights Management ("DRM") technology.[145]

While the balancing test of my proposed digital fair use exception might prevent some of these problems from occurring in the future, the most recent report produced under § 1201(a)(1)(C)[146] (addressed at length in Part II.E., *infra.*) provides four exemptions which I have incorporated in my proposal: i) §§ 1201A(d)(8) (filtering software), ii) (9) (defective dongles), iii) (10) (software contained on media which can only be accessed via obsolete hardware) and iv) (11) (eBook access for handicapped users).[147]

E. *Congress Is Back In Charge*

Even while adopting the above-mentioned exemptions that result from the most recent administrative rulemaking, this proposal attempts to address the concerns articulated by David Nimmer in his article, "Back From the Future: A Proleptic Review of the Digital Millennium Copyright Act":

But already by 2000, the Copyright Office recognized how unwieldy was the task that the DMCA assigned to it. It complained that "the Commerce Committee Report does not state how future adverse impacts are to be evaluated." Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64555, 64559 (Oct. 27, 2000). It further quoted a leading proponent of exemptions as admitting that "the inquiry into whether users of copyrighted works are likely to be adversely effected by the full implementation of section 1201(a)(1) is necessarily 'speculative

---

[145] [T]he effects of existing laws intended to protect digital content, are quite direct in limiting research. For example, the DMCA's strictures regarding anti-circumvention measures have been read to discourage reverse engineering—a technique that has traditionally been used in the high-tech area, perhaps most intensely in the videogame industry, to facilitate the development of new products and services. Ironically, the DMCA may also be inhibiting research about ways of making information more secure. While the DMCA includes an exemption for certain research regarding encryption, at least one noted researcher in the area was reminded by the Record Industry Association of American that he might be sued under the DMCA for disclosure at an academic meeting of encryption researchers of his findings that the methods proposed by the RIAA for securing music were, in fact, insecure.

Id. at 32.

[146] *See* Memorandum from Marybeth Peters, Register of Copyrights, to James H. Billington, Librarian of Congress, *available at* http://www.copyright.gov/1201/ docs/registers-recommendation.pdf (Oct. 27, 2003). *See* discussion *infra* Part E.

[147] *See infra* Appendix B for full text of these exemptions. This proposal adopts the full language of the Register's Recommendation. With respect to the reasoning behind each of these exemptions, see *supra* note 152.

since it entails a prediction about the future.'" Id. at 64562-63 (quoting Peter Jaszi).[148]

Additionally, several concerns have been raised during the rulemaking process itself. The degree of proof required has proved to be unduly burdensome, thus limiting the numbers of classes of works which find exemptions under this scheme. On August 11, 2003, in fulfilling the "consultation" requirement of a § 1201(a)(1)(C) proceeding, Nancy Victory of the Department of Commerce publicly issued a letter to Register of Copyrights Marybeth Peters.[149] In it, she noted that the rulemaking notice of inquiry required aggrieved users to demonstrate a *substantial* burden on fair use rights, a standard not called for in the statute.[150] Similarly, the letter criticized the requirement of "first-hand" knowledge of adverse effects when they were offered under the statute's "likely to produce adverse impacts" standard.[151] Finally, a critique requesting greater specificity in defining what exactly constitutes a "particular class of works" for purpose of the rulemaking was sought.[152]

In response to these critiques, and in an attempt to return full control of (at least this aspect of) copyright law to Congress rather than the administrative process, I propose that §§ 1201(a)(1)(B)-(E) be deleted and replaced with my proposed §§ 1201A(a)-(c),[153] which includes the following changes. First, all of the factors to be considered in the rulemaking should be evaluated under the standard of "any likely or actual effect which is or may be greater than de minimis," thus addressing concerns over previous requirements for first-hand knowledge and substantial burdens on fair use rights prior to adoption in the Register's Recommendation. Second, rather than existing as federal regulations, findings of detrimental effects in the notice and comment proceeding should be factors in the § 1201A(e) digital fair use inquiry, until enacted fully by Congress as exemptions.

F. *The Trade-Off: Tightening the Screws on Infringers*

Unlike the changes suggested in Parts II.B.-D. of this paper, however, the effect of reducing the results of administrative proceedings

---

[148] David Nimmer, *Back From the Future: A Proleptic Review of the Digital Millennium Copyright Act*, 16 BERKELEY TECH. L.J. 855, 870 (2001).

[149] Letter from Nancy Victory, Assistant Secretary of the Department of Commerce, to Marybeth Peters, Register of Copyrights, *available at* http://www.ntia.doc.gov/ntiahome/occ/dmca/dmca2003/dmcaletter_08112003.html (Aug. 11, 2003).

[150] *Id.*

[151] *Id.*

[152] *Id.*

[153] *See infra* Appendix B for full text.

from regulations with the force of law to factors to consider in a balancing test tilts in favor of the content industry. Throughout, this proposal has attempted to realign the equities that appeared off-kilter in § 1201. As such, one other major change also serves to ensure the balance does not tip too strongly in favor of the users of digital works.

In "A Riff on Fair Use," David Nimmer posed the following question: "Why is it that section 1201 is drafted . . . to set forth both an underlying basic provision and a complementary trafficking ban without any comparable underlying provision corresponding to its additional violations?"[154] The answer he provides, from the legislative history, is that copyright law already protects copyright violations (which are similarly protected by the technologies that cannot be circumvented under § 1201(b)), and hence, further *legal* protection is unnecessary.[155] Also, as noted in Part II.C., *supra*, the courts have explained this oddity by saying the presence of a parallel user-side ban to the circumvention of copyright protections would adversely impact fair use rights.[156]

However, even the pro-consumer DCC reports the need for strong legal protections[157] and the validity of including technological means (specifically, watermarking technology)[158] to defend against infringement. In adopting this normative belief, and to continue to foster the growth in technologies that protect copyright rights, I propose a user-side ban in § 1201(b) that parallels the similar ban in § 1201(a):

> (b) Copyright control circumvention violations.—
> (1)
> (A) No person shall circumvent a technological measure that effectively protects a right of a copyright owner under this title in a work.
> (B) A violator of subparagraph (A) shall be subject to double the money damages otherwise available under Chapter 5 or section 1203 of this title.

---

[154] NIMMER, *supra* note 48, at 691.

[155] *Id.*

[156] Universal City Studios, Inc. v. Corley, 273 F.3d 429, 443 (2d Cir. 2001); 321 Studios v. MGM Studios, Inc., 307 F. Supp. 2d 1085, 1097-98 (N.D. Cal. 2004); United States v. Elcom, Ltd., 203 F. Supp. 2d 1111, 1134 (N.D. Cal. 2002).

[157] We see no reason why the content industry should not use [civil and criminal penalties and remedies of Title 17]; particularly as the greatest threats to industry revenues (up to two-thirds of all losses due to piracy) are from commercially driven pirates duplicating physical media such as tapes and CDs. Such large-scale offenders should be the subjects of lawsuits—and we do not think that the content industry will alienate the mass market by going after true pirates.

DCC Report, *supra* note 20, at 49-50.

[158] *Id.* at 28-29.

> (C) Any valid defense to copyright infringement under this title shall also serve as a defense to a violation of subparagraph (A).

In this subsection, subparagraph (B) adds bite to this restriction.[159] Now an individual user can be put on the hook for serious damages.[160] However, no similar bite is needed for § 1201(a)(1) because that balance has not similarly been upset in this proposal.

Further, subparagraph (C) addresses the concerns that to afford legal meaning to technological copyright protections would be to erase an individual's fair use rights. Under this provision, a valid fair use defense with respect to the underlying work would absolve the defendant from any liability for a § 1201(b)(1) violation.

CONCLUSION

My proposed alterations to § 1201 aim to restore the balance in copyright law that appears to have been offset by the early years of the statute's application. Fair use as a defense is protected, and users are once again entitled to find tools which enable fair use to take place. Both copyright holders and technologists are encouraged to find ways to move technology forward while respecting each others' rights and meeting legitimate consumer expectations. The public domain remains a vibrant source of material on which to build. Finally, copyright law is once again the province of legislation without the spectre of complex administrative regulation excessively complicating the matter.

---

[159] Although 17 U.S.C. § 1203 (2004) had previously addressed all remedies for violations of 17 U.S.C. § 1201 (2004), it is worth noting that even 17 U.S.C. § 1201(d)(1)(C) (2004) contains language triggering remedies in some cases.

[160] While it may, in practice, be difficult to actually catch a defendant for violations of the copy control aspects of, for example, CSS, other in-development technologies such as watermarking, when combined with the MPAA's internet investigations unit, can indeed be used to track down individual infringers. In fact, such an event took place this year, when the source of a decrypted Academy screener copy of "Something's Gotta Give" that appeared online was successfully traced to its source. "Arrest in movie bootlegging scheme," (2004) *available at* http://www.cnn.com/2004/SHOWBIZ/01/23/oscar.arrest/index.html.

APPENDICES

Appendix A: § 1201

§ 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.

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

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

(i) the availability for use of copyrighted works;

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

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

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

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

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

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

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

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

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

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

(3) As used in this subsection—

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

(B) a technological measure "effectively controls access to a work" if the measure, in the ordinary course of its operation, requires the application of information, or a process

or a treatment, with the authority of the copyright owner, to gain access to the work.

(b) Additional violations.—

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

(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;

(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

(2) As used in this subsection—

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

(B) a technological measure "effectively protects a right of a copyright owner under this title" if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title.

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

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

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

(3) Nothing in this section shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure, so long

as such part or component, or the product in which such part or component is integrated, does not otherwise fall within the prohibitions of subsection (a)(2) or (b)(1).

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

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

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

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

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

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

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

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

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

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

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

(A) open to the public; or

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

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

(f) Reverse engineering.—

(1) Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.

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

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

(4) For purposes of this subsection, the term "interoperability" means the ability of computer programs to exchange informa-

tion, and of such programs mutually to use the information which has been exchanged.

(g) Encryption research.—

(1) Definitions.—For purposes of this subsection—

(A) the term "encryption research" means activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products; and

(B) the term "encryption technology" means the scrambling and descrambling of information using mathematical formulas or algorithms.

(2) Permissible acts of encryption research.—Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if—

(A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work;

(B) such act is necessary to conduct such encryption research;

(C) the person made a good faith effort to obtain authorization before the circumvention; and

(D) such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

(3) Factors in determining exemption.—In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include—

(A) whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under this title or a violation of applicable law other than this section [17 U.S.C.A. § 1 et seq.], including a violation of privacy or breach of security;

(B) whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology; and

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

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

(A) develop and employ technological means to circumvent a technological measure for the sole purpose of that person performing the acts of good faith encryption research described in paragraph (2); and

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

(5) Report to Congress.—Not later than 1 year after the date of the enactment of this chapter [17 U.S.C. § 1201 et seq.], the Register of Copyrights and the Assistant Secretary for Communications and Information of the Department of Commerce shall jointly report to the Congress on the effect this subsection has had on—

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

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

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

The report shall include legislative recommendations, if any.

(h) Exceptions regarding minors.—In applying subsection (a) to a component or part, the court may consider the necessity for its intended and actual incorporation in a technology, product, service, or device, which—

(1) does not itself violate the provisions of this title; and

(2) has the sole purpose to prevent the access of minors to material on the Internet.

(i) Protection of personally identifying information.—

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

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

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

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

(D) the act of circumvention is carried out solely for the purpose of preventing the collection or dissemination of personally identifying information about a natural person who seeks to gain access to the work protected, and is not in violation of any other law.

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

(j) Security testing.—

(1) Definition.—For purposes of this subsection, the term "security testing" means accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network.

(2) Permissible acts of security testing.—Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to engage in an act of security testing, if such act does not constitute infringement under this title or a

violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

(3) Factors in determining exemption.—In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include—

(A) whether the information derived from the security testing was used solely to promote the security of the owner or operator of such computer, computer system or computer network, or shared directly with the developer of such computer, computer system, or computer network; and

(B) whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security.

(4) Use of technological means for security testing.— Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to develop, produce, distribute or employ technological means for the sole purpose of performing the acts of security testing described in subsection (2), provided such technological means does not otherwise violate section (a)(2).

(k) Certain analog devices and certain technological measures.—

(1) Certain analog devices.—

(A) Effective 18 months after the date of the enactment of this chapter, no person shall manufacture, import, offer to the public, provide or otherwise traffic in any—

(i) VHS format analog video cassette recorder unless such recorder conforms to the automatic gain control copy control technology;

(ii) 8mm format analog video cassette camcorder unless such camcorder conforms to the automatic gain control technology;

(iii) Beta format analog video cassette recorder, unless such recorder conforms to the automatic gain control copy control technology, except that this requirement shall not apply until there are 1,000 Beta format analog video cassette recorders sold in the United States in any one calendar year after the date of the enactment of this chapter;

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

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

(B) Effective on the date of the enactment of this chapter, no person shall manufacture, import, offer to the public, provide or otherwise traffic in—

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

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

Manufacturers that have not previously manufactured or sold a VHS format analog video cassette recorder, or an 8mm format analog cassette recorder, shall be required to conform to the four-line colorstripe copy control technology in the initial model of any such recorder manufactured after the date of the enactment of this chapter, and thereafter to continue conforming to the four-line colorstripe copy control technology. For purposes of this subparagraph, an analog video cassette recorder "conforms to" the four-line colorstripe copy control technology if it records a signal that, when played back by the playback function of that recorder in the normal viewing mode, ex-

hibits, on a reference display device, a display containing distracting visible lines through portions of the viewable picture.

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

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

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

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

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

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

(3) Inapplicability.—This subsection shall not—

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

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

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

(4) Definitions.—For purposes of this subsection:

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

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

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

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

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

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

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

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

APPENDIX B: AUTHOR'S PROPOSED §§ 1201 AND 1201A

§ 1201. CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS

(a) Violations regarding circumvention of technological measures.—
  (1) 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 apply to all covered activities commencing on or after October 28, 2000, unless covered by an exemption described in section 1201A.
  (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, unless an exemption or defense under ; and
    (B) has no substantial noninfringing 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.

    unless an exemption or defense under § 1201A applies.
  (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;
    (B) "access" means the ability to perceive a writing, audiovisual work, performance or phonogram, or to manually execute a computer software application; and
    (C) 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) Copyright control circumvention violations.—
  (1)

(A) No person shall circumvent a technological measure that effectively protects a right of a copyright owner under this title in a work.

(B) A violator of subparagraph (A) shall be subject to double the money damages otherwise available under Chapter 5 or section 1203 of this title.

(C) Any valid defense to copyright infringement under this title shall also serve as a defense to a violation of subparagraph (A).

(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) has no substantial noninfringing 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

(B) 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.

unless an exemption or defense under § 1201A applies.

(3) 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, including but not limited to the exclusive rights to copy, distribute, or create derivative works.

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

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

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

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

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

(d) Anticircumvention misuse.

(1) The bundling of works which reside in the public domain, or which are otherwise not protected by this title, and which are not reasonably available in another form by potential users of those works, within an access control subject to subsection (a) of this section, shall constitute "anticirumvention misuse," and shall bar a plaintiff from bringing any action under this section.

(2) Works shall be deemed "reasonably available in another form" within the meaning of paragraph (1) if the producer or marketer of the work which would otherwise fall with the bar of paragraph (1) includes a method of accessing the unprotected works in the user interface which is readily accessible by any potential user.

(3) Anticircumvention misuse as defined in this subsection shall not serve as a defense to the infringement of any other right protected by this title.

(e) Certain analog devices and certain technological measures.—

(1) Certain analog devices.—

(A) Effective 18 months after the date of the enactment of this chapter, no person shall manufacture, import, offer to the public, provide or otherwise traffic in any—

(i) VHS format analog video cassette recorder unless such recorder conforms to the automatic gain control copy control technology;

(ii) 8mm format analog video cassette camcorder unless such camcorder conforms to the automatic gain control technology;

(iii) Beta format analog video cassette recorder, unless such recorder conforms to the automatic gain control copy control technology, except that this requirement shall not apply until there are 1,000 Beta format analog video cassette recorders sold in the United States

in any one calendar year after the date of the enactment of this chapter;

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

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

(B) Effective on the date of the enactment of this chapter, no person shall manufacture, import, offer to the public, provide or otherwise traffic in—

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

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

Manufacturers that have not previously manufactured or sold a VHS format analog video cassette recorder, or an 8mm format analog cassette recorder, shall be required to conform to the four-line colorstripe copy control technology in the initial model of any such recorder manufactured after the date of the enactment of this chapter, and thereafter to continue conforming to the four-line colorstripe copy control technology. For purposes of this subparagraph, an analog video cassette recorder "conforms to" the four-line color-

stripe copy control technology if it records a signal that, when played back by the playback function of that recorder in the normal viewing mode, exhibits, on a reference display device, a display containing distracting visible lines through portions of the viewable picture.

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

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

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

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

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

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

(3) Inapplicability.—This subsection shall not—

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

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

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

(4) Definitions.—For purposes of this subsection:

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

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

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

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

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

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

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

(5) Violations.—Any violation of paragraph (1) of this subsection shall be treated as a violation of subsection (b)(1) of this section. Any violation of paragraph (2) of this subsection shall be

deemed an "act of circumvention" for the purposes of section 1203(c)(3)(A) of this chapter.

§ 1201A. Exemptions to Section 1201

(a) The protections otherwise afforded by section 1201 shall not apply to the particular classes of works, users, or situations described in subsection (d) subject to the limitations contained therein.

(b) During each succeeding 3-year period after October 28, 2000, the Librarian of Congress shall recommend to Congress amendments to subsection (d) of this section. In formulating this recommendation, the Librarian of Congress shall obtain the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and shall conduct a notice and comment proceeding to determine whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibitions of section 1201 in their ability to make noninfringing uses under this title of a particular class of copyrighted works. In drafting the recommendation, the Librarian shall examine the effects during the current three year period, and the potential effects during the succeeding three year period, of the following —
   (1) any likely or actual effect which is or may be greater than de minimis on the availability for use of copyrighted works;
   (2) any likely or actual effect which is or may be greater than de minimis on the availability for use of works for nonprofit archival, preservation, and educational purposes;
   (3) any likely or actual effect which is or may be greater than de minimis on impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;
   (4) any likely or actual effect which is or may be greater than de minimis on effect of circumvention of technological measures on the market for or value of copyrighted works;
   (5) any likely or actual effect which is or may be greater than de minimis on the availability of works in the public domain or otherwise not protected under this title; and
   (6) such other factors as the Librarian considers appropriate.

(c) The Librarian shall publish any class of copyrighted works for which the Librarian has determined, pursuant to the procedures conducted under paragraph (b), that noninfringing uses by persons

who are users of a copyrighted work are, or are likely to be, adversely affected, the findings of which shall be considered as one factor in the defense established by subsection (e) of this section in any action under the prohibitions contained in section 1201 for the ensuing 3-year period, pending Congressional adoption in paragraph (d) of this subsection.

(d) Specific Exemptions

(1) Libraries and Archives

(A) A nonprofit library, archives, or educational institution which gains access to a commercially exploited copyrighted work solely in order to make a good faith determination of whether to acquire a copy of that work for the sole purpose of engaging in conduct permitted under this title shall not be in violation of sections 1201(a)(1) or 1201(b)(1). A copy of a work to which access has been gained under this paragraph may not be retained longer than necessary to make such good faith determination; and may not be used for any other purpose.

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

(C) A nonprofit library, archives, or educational institution that willfully for the purpose of commercial advantage or financial gain violates this paragraph —

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

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

(D) This subsection may not be used as a defense to a claim under section 1201(a)(2) or 1201(b)(2).

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

(i) open to the public; or

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

(2) Law enforcement, intelligence, and other government activities.—This section does not prohibit any lawfully authorized investigative, protective, information security, or intelligence

activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State. For purposes of this subsection, the term "information security" means activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network.

(3) Reverse engineering.—

(A) Notwithstanding the provisions of sections 1201(a)(1) and 1201(b)(1), 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.

(B) Notwithstanding the provisions of sections 1201(a)(2) and 1201(b)(2), 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 subparagraph (A), 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.

(C) The information acquired through the acts permitted under subparagraph (A), and the means permitted under subparagraph (B), may be made available to others if the person referred to in subparagraphs (A) or (B), 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.

(D) For purposes of this subsection, the term "interoperability" means the ability of computer programs to ex-

change information, and of such programs mutually to use the information which has been exchanged.

(4) Encryption research.—

(A) Definitions.—For purposes of this subsection—

(i) the term "encryption research" means activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products; and

(ii) the term "encryption technology" means the scrambling and descrambling of information using mathematical formulas or algorithms.

(B) Permissible acts of encryption research.—Notwithstanding the provisions of section 1201(a)(1), it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if—

(i) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work;

(ii) such act is necessary to conduct such encryption research;

(iii) the person made a good faith effort to obtain authorization before the circumvention; and

(iv) such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

(C) Factors in determining exemption.—In determining whether a person qualifies for the exemption under subparagraph (B), the factors to be considered shall include—

(i) whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under this title or a violation of applicable law other than

this section [17 U.S.C.A. § 1 et seq.], including a violation of privacy or breach of security;

(ii) whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology; and

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

(D) Use of technological means for research activities.—Notwithstanding the provisions of section 1201(a)(2), it is not a violation of that subsection for a person to—

(i) develop and employ technological means to circumvent a technological measure for the sole purpose of that person performing the acts of good faith encryption research described in subparagraph (B); and

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

(5) Exceptions regarding minors.—In applying section 1201(a) to a component or part, the court may consider the necessity for its intended and actual incorporation in a technology, product, service, or device, which—

(A) does not itself violate the provisions of this title; and

(B) has the sole purpose to prevent the access of minors to material on the Internet.

(6) Protection of personally identifying information.—

(A) Circumvention permitted.—Notwithstanding the provisions of section 1201(a)(1), it is not a violation of that subsection for a person to circumvent a technological measure that effectively controls access to a work protected under this title, if—

(i) the technological measure, or the work it protects, contains the capability of collecting or disseminating personally identifying information reflecting the on-

line activities of a natural person who seeks to gain access to the work protected;

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

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

(iv) the act of circumvention is carried out solely for the purpose of preventing the collection or dissemination of personally identifying information about a natural person who seeks to gain access to the work protected, and is not in violation of any other law.

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

(7) Security testing.—

(A) Definition.—For purposes of this subsection, the term "security testing" means accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network.

(B) Permissible acts of security testing.—Notwithstanding the provisions of section 1201(a)(1), it is not a violation of that subsection for a person to engage in an act of security testing, if such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

(C) Factors in determining exemption.—In determining whether a person qualifies for the exemption under paragraph (B), the factors to be considered shall include—

(i) whether the information derived from the security testing was used solely to promote the security of the owner or operator of such computer, computer system or computer network, or shared directly with the developer of such computer, computer system, or computer network; and

(ii) whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security.

(D) Use of technological means for security testing.—Notwithstanding the provisions of section 1201(a)(2), it is not a violation of that subsection for a person to develop, produce, distribute or employ technological means for the sole purpose of performing the acts of security testing described in paragraph (B), provided such technological means does not otherwise violate section 1201(a)(2).

(8) Filtering software.— It shall not be a violation of section 1201(a)(1) to circumvent an access control on commercially marketed filtering software applications that are intended to prevent access to domains, websites or portions of websites to access a compilation of lists of Internet locations blocked by that software. This exemption does not apply to lists of Internet locations blocked by software applications that operate exclusively to protect against damage to a computer or computer network or lists of Internet locations blocked by software applications that operate exclusively to prevent receipt of email.

(9) Defective dongles.—

(A) It shall not be a violation of section 1201(a)(1) to access lawfully acquired copies of Computer programs protected by malfunctioning or damaged dongles where replacement or repair is not readily available for the dongle due to the obsolescence of its hardware connection, the termination of operations of the manufacturing firm, or a cost in excess of twenty per cent of the initial purchase price of the software package to repair or replace the dongle.

(B) The term "dongle" in subparagraph (A) refers to any hardware device which must be connected to a computer system to enable access to otherwise readable software installed on that system.

(10) Software contained on media which can only be accessed via obsolete hardware.

(A) It shall not be a violation of sections 1201(a)(1) or 1201(b)(1) to access 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. A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial marketplace.

(B) It shall not be a violation of any part of this section or this title to make one archival copy of software as described in subparagraph (A) to a more durable format, provided that any copy made under this protection not be accessed, distributed, or otherwise modified until the obsolescence discussed in subparagraph (A) has occurred.

(C) The protections of subparagraphs (A) and (B) shall not apply to any software title for which the copyright holder has made access via a non-obsolete medium reasonably available.

(11) eBook access for handicapped users—It shall not be a violation of sections 1201(a)(1) or 1201(b)(1) of this title to access Literary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling of the ebook's read-aloud function and that prevent the enabling of screen readers to render the text into a specialized format where the access is gained by or for the use of the owner of a lawfully acquired digital copy who is visually impaired or who otherwise suffers from a barrier to normal literacy.

(e) Digital Fair Use

(1) It is not a violation of sections 1201(a)(1) or 1201(b)(1) circumvent a technological measure in connection with access to, or the use of, a work if such circumvention does not result in an infringement of the copyright in the work.

(2) Fair Trafficking

(A) The manufacture, distribution, importation or marketing of a hardware or software product that is reasonably necessary to circumvent an access or copyright protection control as allowed under subsections (d) or (e)(1) shall be considered fair trafficking if that hardware or software product is capable of substantial noninfringing use, and shall not violate sections 1201(a)(1) or 1201(b)(2).

(B) In determining whether or not an act of trafficking is fair within the meaning of paragraph (A), a court shall consider:

(i) the failure, if any, of the copyright holder to make publicly available the necessary means to perform noninfringing uses as described in paragraph (1) without additional cost or burden to the user of the work;

(ii) the extent to which the design and marketing of the product or device challenged under section 1201(a)(2) or 1201(b)(2) is limited to enabling noninfringing uses;

(iii) the reasonableness of the consumer expectations for noninfringing uses which could not be met absent such a product or device;

(iv) the availability and suitability of alternative works or versions of works to the noninfringing uses most likely to be desired by the intended customers of the product or device;

(v) the inclusion or exclusion of the circumvention means or class of works most affected by it in the reports of the Librarian of Congress published under subsection (c); and

(vi) such other factors as the court considers relevant to determining the fairness of barring the trafficking of the specific product.