INTELLECTUAL PROPERTY AND THE DIGITAL ECONOMY: WHY THE ANTI-CIRCUMVENTION REGULATIONS NEED TO BE REVISED

by
Pamela Samuelson*

INTRODUCTION

The Clinton Administration's "Framework For Global Electronic Commerce" aims to promote the development of a vast global market in which electronic contracts will be made for delivery of electronic information products and services via digital networks which will be paid for with electronic currencies.[1] The Framework simultaneously encourages private investment and entrepreneurship, urges governments at all levels to act with restraint in considering regulations of the emerging e-conomy,[2] and argues for international cooperation in adopting consistent policies that will promote this commerce.[3] The Commerce Department's First Annual Report on the Framework initiative indicates that this initiative has met with some success.[4] Passage of the Digital Millenium Copyright Act (DMCA) is among the successes claimed in this report.[5]

The Commerce Department may be correct in thinking that the interests of the digital economy will be furthered by widespread acceptance of the WIPO Copyright Treaty in the international community.[6] This treaty establishes several important international norms for applying copyright law in the digital environment.[7] International consensus on these norms should aid the growth of the global digital economy.[8] However, the DMCA was largely unnecessary because U.S. law already complied with all but one minor provision of the treaty.[9] The DMCA went far beyond treaty requirements as regards the

---

* Professor of Information Management and of Law, University of California at Berkeley; Co-Director of the Berkeley Center for Law and Technology. This paper is an outgrowth of work initially done for an Emory Law School conference on the law of cyberspace held in February 1996. The draft article produced for this conference entitled "Technical Protection for Copyrighted Works" discussed a 1995 legislative proposal for regulating the circumvention of technical protection systems. I am deeply indebted to Benjamin Black who was my research assistant during preparation of this draft. He subsequently collaborated with me on a subsequent draft article on this subject. Although that project was never completed, this article builds on the base of the collaboration with him. I am also grateful for comments on this draft from Hal Abelson, Bob Glushko, Laurel Jamtgaard, and Kurt Opsahl.

[1] *See* WILLIAM J. CLINTON & ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE (1997), *available at* <http://www.iitf.nist.gov/eleccomm/ecomm.htm> (hereinafter "Framework").

[2] I have borrowed the term "e-conomy" from Berkeley colleagues John Zysman and Michael Borrus.

[3] Framework, supra note 1, at 2-4.

[4] U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE, FIRST ANNUAL REPORT, Nov. 1998 (cited hereinafter as "E-Commerce Annual Report").

[5] Pub. L. No. 105-304, mentioned in E-Commerce Annual Report, supra note 4, at 2.

[6] See WIPO Copyright Treaty, Adopted by the Diplomatic Conference, WIPO Doc. CRNR/DC/89 (December 20, 1996) (cited hereinafter as "WIPO Copyright Treaty"). There were actually two treaties concluded at this diplomatic conference. The other was the WIPO Performances and Phonograms Treaty, Adopted by the Diplomatic Conference, WIPO Doc. CRNR/DC/90 (Dec. 20, 1996) (cited hereinafter as "WIPO Phonograms Treaty"). Because the U.S. protects the interests of producers and performers of phonograms largely through copyright law and because the phonograms treaty was not materially different in its requirements as regards issues covered in this article, the article will, for the sake of simplicity, focus on the WIPO Copyright Treaty provisions. See generally Pamela Samuelson, The U.S. Digital Agenda at WIPO, 37 VA. J. INT'L L. 369 (1997) (discussing the negotiations leading to conclusion of the WIPO Copyright Treaty).

[7] See infra notes – and accompanying text for a discussion of these norms.

[8] E-Commerce Annual Report, supra note 4, at 13-14.

[9] See, e.g., Pamela Samuelson, Big Media Beaten Back, 5.03 WIRED 64 (March 1997) (explaining that U.S. law was in compliance with almost all norms of the treaty). Only the treaty provision calling for

regulation of circumvention of technical protection systems used by copyright owners to protect their works.[10]

The anti-circuvmention rules in the DMCA do not match up well with the needs of the digital economy, nor with the principles propounded in the Framework.[11] Although the First Annual report praises DMCA for the balance it embodies,[12] this article will demonstrate that such balance as DMCA contains is attributable to Congressional foresight, not to the Clinton Administration.[13] Indeed, for the past five years, the Administration has supported highly imbalanced digital copyright initiatives and has resisted most efforts to introduce more balance in these initiatives.[14] With the enactment of the anti-circumvention provisions of the DMCA, the Administration may have had more success in maintaining imbalance in digital copyright law than Congress may have realized.[15]

It would oversimplify the facts—although not by much—to say that the battle in Congress over the anti-circumvention provisions of the DMCA was a battle between Hollywood and Silicon Valley.[16] Hollywood and its allies sought the strongest possible ban both of the act of circumventing a technical protection system used by copyright owners to protect their works and of technologies having circumvention-enabling uses.[17] Silicon Valley firms and their allies opposed this broad legislation because of deleterious effects it would have on their ability to engage in lawful reverse engineering, computer security testing, and encryption research.[18] They supported legislation to outlaw acts of circumvention engaged in for the purpose of infringing copyrights and would have supported narrowly drawn device

---

protecting the integrity of rights management information needed legislative implementation in U.S. law. WIPO Copyright Treaty, supra note 6, Art. 12. See also infra notes—and accompanying text.

[10] WIPO Copyright Treaty, supra note 6, Art. 11. The DMCA anti-circumvention provision can be found at 17 U.S.C. sec. 1201. See infra notes – and accompanying text for a discussion of why the treaty did not require the DMCA provisions.

[11] See Section II for an articulation of these principles. See Sections IV-VII for an analysis of why these provisions may be harmful to digital economy interests.

[12] E-Commerce Annual Report, supra note 4, at 14.

[13] See Section IV.

[14] See REPORT OF WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS OF INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY RIGHTS AND THE NATIONAL INFORMATION INFRASTRUCTURE (Sept. 1995) (cited hereinafter as "White Paper"). Numerous articles have criticized this and an earlier draft report because of its imbalance heavily tilted in favor of publisher interests. See, e.g., Peter A. Jaszi, Caught in the Net of Copyright, 75 ORE. L. REV. 299 (1996); Leslie Kurtz, Copyright and the National Information Infrastructure, 18 EUR. INTELL. PROP. REV. 120 (1996); Jessica Litman, The Exclusive Right to Read, 13 CARDOZO ARTS & ENT. L. 29 (1994); Charles R. McManis, Taking TRIPS on the Information Superhighway: International Intellectual Property and Emerging Computer Technology, 41 VILL. L. REV. 207 (1996); Pamela Samuelson, The Copyright Grab, 4.01 WIRED 134 (Jan. 1996). Such balance as exists in the anti-circumvention regulations derives largely from the Commerce Committee in the House of Representatives and from the Senate Judiciary Committee. See infra notes – and accompanying text for a further discussion of the evolution of these provisions.

[15] See Section VI.

[16] See, e.g., Testimony of Jack Valenti on behalf of Motion Picture Association of America and Testimony of Edward J. Black on behalf of the Computer & Communications Industry Ass'n , Hearing Before the Subcommittee on Courts and Intellectual Property of the House Judiciary Committee on H.R. 2281, 105th Cong., 2d Sess., September 17, 1997 (these testimonies are cited hereinafter respectively "Valenti Testimony" and "Black Testimony," and the September hearing as "House Jud. Hearing"). It should be noted that the Business Software Alliance, whose principal member is Microsoft, supported Hollywood's preferred bill for reasons which may become apparent infra notes – and accompanying text. See Testimony of Robert Holleyman, House Jud. Hearing.

[17] Valenti Testimony, supra note 16. See also Testimony of Allan R. Adler on behalf of the Association of American Publishers, House Jud. Hearing, supra note 16.

[18] See infra notes – and accompanying text. Other groups opposed to the broad anti-circumvention legislation of H.R. 2281 included librarians and educators. See infra notes – and accompanying text.

legislation had the Congressional subcommittees principally responsible for formulating WIPO treaty implementation legislation been receptive to a narrower bill.[19] Silicon Valley and its allies warned of dire consequences if the overbroad anti-circumvention provisions Hollywood supported were adopted.[20] Yet, by colorful use of high rhetoric and forceful lobbying, Hollywood and its allies were successful in persuading Congress to adopt the broad anti-circumvention legislation they favored, even if it is now subject to some specific exceptions that respond to some concerns raised by Silicon Valley firms and their allies in the legislative process.[21]

Had the Administration sought to broker a fairer compromise between the interests of Hollywood and its allies and the interests of the Silicon Valley and its allies, this process would almost certainly have produced better legislation than the anti-circumvention provisions of the DMCA. One would have thought, given the Framework's principles and the Administration's enthusiasm for the strong economic performance of the information technology sector, that the Administration would have taken a more balanced position on these issues.[22] One can call the DMCA's anti-circumvention provisions many things, but one cannot honestly speak of them as "predictable, minimalist, consistent, and simple" components of a legal environment for electronic commerce, as the Framework principles would suggest they should be.[23]

This article will make three main points about the anti-circumvention rules in the DMCA. First, there are far more legitimate reasons to circumvent a technical protection system than the DMCA anti-circumvention act provisions expressly recognize.[24] The legislation should be amended to provide a general purpose "or other legitimate purposes" provision to avert judicial contortions in interpreting the statute. Second, the anti-device provisions of the DMCA are highly ambiguous and overbroad, raising questions about whether Congress understood the potential for these provisions to undermine circumvention privileges built into the anti-circumvention act provision.[25] The anti-device provisions of DMCA should be clarified and a more minimalist approach taken to the regulation of technologies with circumvention-enabling uses so that the ambiguity and overbreadth of the existing provisions will not cause harm to innovation and competition in the information technology sector. Third, at the very least, periodic reviews of the impact of the anti-circumvention provisions of the DMCA should be undertaken.[26] Given how broad the anti-circumvention rules are, given their unprecedented character, and given the potential for mischief from these rules already evident from the legislative record, Congress should authorize a far broader study of the impact of these provisions than the DMCA presently contemplates. It should also heed proposals for change to the anti-circumvention provisions recommended in such studies.

I. THE DIGITAL ECONOMY IS A HIGH GROWTH, HIGH POTENTIAL SECTOR WHOSE NEEDS DESERVE CAREFUL CONSIDERATION.

An April 1998 report on "The Emerging Digital Economy" published by the U.S. Department of Commerce begins with the following observations:

---

[19] The Digital Future Coalition whose members include the Computer & Communications Industry Association, among other high tech industry groups, endorsed H.R. 3048, 105th Cong., 2d Sess. (1997) which proposed such a narrow circumvention provision. See 55 BNA Pat., Trademark, & Cop. J. 70-71 (description of the anti-circumvention provision of H.R. 3048). See also Black Testimony, supra note 16 (critical of the Administration's anti-circumvention proposal); Testimony of Chris Byrne on behalf of the Information Technology Industry Association, House Jud. Hearing, supra note 16 (critical of H.R. 2281).

[20] See, e.g., Black Testimony, supra note 16, at [5-6]. See also Testimony of Robert Oakley, House Jud. Hearing., supra note 16.

[21] See Section IV.

[22] See Section II.

[23] Framework, supra note 1, at 3. For further criticism of the DMCA's anti-circumvention provisions on constitutional grounds, see Yochai Benkler, Free As the Air To Common Use: First Amendment Constraints on the Enclosure of the Public Domain, N.Y.U. L. REV. (forthcoming 1999).

[24] See Section V.

[25] See Section VI.

[26] See Section VII.

> During the past few years, the United States economy has performed beyond most expectations. A shrinking deficit, low interest rates, a stable macroeconomic environment, expanding international trade with few barriers, and effective private sector management are all credited with playing a role in this healthy economic performance.
>
> Many observers believe advances in information technology (IT) driven by the growth of the Internet have also contributed to a healthier-than-expected economy.
>
> In recent testimony to Congress, Federal Reserve Board Chairman Alan Greenspan noted, "our nation has been experiencing a higher growth rate of productivity—output per hour worked—in recent years. The dramatic improvements in information technology appear to have been a major force behind this beneficial trend.[27]

This report indicates that the IT sector of the U.S. economy—which includes the computer hardware, software, networking and telecommunications industries—now constitutes 8.2 per cent of the gross domestic product, close to twice its share of GDP as compared with a decade or so before.[28] The IT sector, moreover, accounts for more than one-quarter of the real economic growth in the American economy.[29] Approximately 45 per cent of current expenditures on business equipment are investments in IT products and services.[30] It is no wonder, then, that the collective capitalization of five major firms in this sector—Microsoft, Intel, Compaq, Dell, and Cisco Systems—has grown from $12 billion in 1987 to $588 billion in 1997, a fifty-fold increase in only a decade.[31] Perhaps somewhat more wonderous are the astonishing market capitalizations of relatively new Internet firms, such as Amazon, Yahoo, and E-Trade; yet, these valuations reflect the market's belief in the high growth potential of these players in the digital economy, even if their earnings so far might seem to belie this.[32] It is, of course, important to realize that the IT sector is not the only component of the digital economy.[33] It is, however, a significant part of that economy, and it is also the enabler of growth in other parts of the digital economy, as vendors of products and services of both tangible and intangible kinds make use of digital networks to offer their wares to a global market.[34] Especially as electronic commerce via the Internet and the World Wide Web expands, the IT sector is likely to experience further explosive growth.[35]

"The Emerging Digital Economy" report continues along the path set by the Administration's early policy document, "The Framework for Global Electronic Commerce," in seeking to foster achieving the growth potential of the digital economy.[36] Both documents recognize that "[g]overnments can have a profound effect on the growth of commerce on the Internet. By their actions, they can facilitate electronic trade or inhibit it. Knowing when to act and—at least as important—when not to act, will be crucial to the development of electronic commerce."[37] One of the signal achievements of the Framework was the promulgation of five principles which were supposed to guide U.S. as well as other governmental action on policy initiatives on electronic commerce:

(1) The private sector should lead.
(2) Governments should avoid undue restrictions on electronic commerce.

---

[27] U.S. DEPT. OF COMMERCE, SECRETARIAT ON ELECTRONIC COMMERCE, THE EMERGING DIGITAL ECONOMY at 1 (April 1998) (hereinafter "Emerging Digital Economy").
[28] Id. at 4.
[29] Id. at 6.
[30] Id.
[31] Id. Of course, it is fair to observe that some of this growth has occurred by virtue of acquisitions of other substantial firms, such as Compaq's acquisition of Digital Equipment Corp.
[32] See, e.g., Steve Mott, Where Eagles Soar: Making Sense of Internet Valuations, BUSINESS 2.0 (Nov. 1998).
[33] Emerging Digital Economy, supra note 26, Chap. 4-5 (discussing digital economy sectors).
[34] Id.
[35] Id.
[36] Id. at 50-51.
[37] Framework, supra note 1, at 3. Emerging Digital Economy, supra note 26, at 50-51.

(3) Where government involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent, and simple legal environment for commerce.
(4) Governments should recognize the unique qualities of the Internet.
(5) Electronic commerce over the Internet should be facilitated on a global basis.[38]

The Framework announced nine policy areas in which it said it would apply these principles: customs and taxation, electronic payment systems, commercial law, intellectual property protection, privacy, security, telecommunications infrastructure, content, and technical standards.[39] The "First Annual Report" of the U.S. Working Group on Electronic Commerce has added five other policy initiatives to the list,[40] and offers evidence that the Framework's policy objectives are being achieved.[41]

As laudable as the Framework's principles are, it should be said that the Clinton Administration has been somewhat erratic in following them. The Administration has a good record in promoting minimalist tax and customs policies.[42] However, it has been widely criticized by the information technology/digital economy sector for not following these principles in the security/encryption policy area and in the content policy area (on account of the Administration's support for the Communications Decency Act).[43] In the legislative struggle leading up to adoption of the DMCA, the Administration deviated from these principles once again in heeding the desires of established copyright industries to restructure the legal infrastructure of the digital environment so that it would accommodate their preferences. These industries insisted that this restructuring was necessary to induce them to participate in the digital economy.[44] Many significant players in the existing digital economy counseled against this restructuring.[45] The Administration should, of course, have considered the interests and concerns of Hollywood and other copyright industry groups in its consideration of an appropriate digital copyright policy initiative. However, the Administration might have done more to consider the interests of those already participating in the digital economy in its policy formation on these issues, particularly since its preferred policy so clearly violated the principles that the Administration had asserted it would follow.

II. THE WIPO COPYRIGHT TREATY IS GOOD FOR THE NEW ECONOMY.

The WIPO Copyright Treaty established several norms about applying copyright law in the digital environment.[46] They include:

(1) copyright owners should have an exclusive right to control the making of copies of their works in digital form,[47]

---

[38] Framework, supra note 1, at 3-4.
[39] Id. at 1.
[40] E-Commerce Annual Report, supra note 4, at 4.
[41] Id. at 2-4.
[42] Id. at 2 (mentioning passage of the Internet Tax Freedom Act) and at 12 (discussing foreign tax initiatives).
[43] See, e.g., ESTHER DYSON, RELEASE 2.0 (1997).
[44] See Valenti Testimony, supra note 16.
[45] See Black Testimony, supra note 16; Byrne Testimony, supra note 18. See also Hearing Before the Subcommittee on Telecommunications, Trade, and Consumer Protection of the House Commerce Committee on H.R. 2281, 105th Cong., 2d Sess., June 5, 1998.
[46] See WIPO Copyright Treaty, supra note 6. See also US Digital Agenda, supra note 6 (discussing the digital agenda WIPO treaty provisions)
[47] There was an explicit provision on the reproduction right in the draft treaty initially considered at WIPO. However, this provision did not attract consensus because of its inclusion of temporary reproductions which was highly controversial. Instead, the diplomatic conference agreed on certain statements of interpretation of the treaty which included a provision on the reproduction right. See Agreed Statements Concerning the WIPO Copyright Treaty, adopted by the Diplomatic Conference on December 20, 1996, WIPO Doc. CRNR/DC/96 at 1 (cited hereinafter as "Agreed Statements"). For a discussion of the tortured history of the draft treaty provision, the Agreed Statements, and what they mean, see, e.g., US Digital Agenda, supra note 6, at 382-92.

(2) copyright owners should have an exclusive right to control the communication of their works to the public,[48]
(3) countries can continue to apply existing exceptions and limitations, such as fair use, as appropriate in the digital environment, and can even create new exceptions and limitations appropriate to the digital environment,[49]
(4) merely providing facilities for the communication of works should not be a basis for infringement liabililty,[50]
(5) it should be illegal to tamper with copyright management information insofar as this would facilitate or conceal infringement in the digital environment,[51] and
(6) countries should have "adequate legal protection and effective legal remedies against the circumvention of effective technological measures" used by copyright owners to protect their works from unauthorized uses.[52]

Insofar as uncertainties about how copyright law should apply in the digital environment were impeding investments in or the growth of a global market in electronic intellectual property products,[53] there was reason to be optimistic that conclusion of this treaty would remove these blockages and allow e-

[48] WIPO Copyright Treaty, Article 8. While the United States does not have an exclusive right of communication in its copyright law, see 17 U.S.C. sec. 106 (exclusive rights provisions), its public performance and distribution rights are substantively equivalent to this right. Id. See US Digital Agenda at WIPO, supra note 6, at 392-98 (discussing negotiations concerning digital communications).
[49] Agreed Statements, supra note 45, at 2. This agreed statement was in striking contrast to the proposed treaty language and proposed comments on exceptions and limitations to copyright in the draft treaty considered at the WIPO diplomatic conference. See US Digital Agenda, supra note 6, at 409 (discussing the draft and final provisions on fair use and other exceptions). Although the White Paper had expressed doubts about the viability of fair use in the digital environment, the Clinton Administration was ultimately persuaded that the WIPO Copyright Treaty should contain a more positive statement about fair use in the digital environment. See White Paper, supra note 14, at 82; US Digital Agenda, supra note 6, at 406.
[50] Agreed Statements, supra note 45, at 2. This issue had been highly contentious, both in the U.S. and at the diplomatic conference, because the Clinton Administration supported holding online service providers strictly liable for infringing acts of their users. See White Paper, supra note 14, at 114-24; US Digital Agenda, supra note 6, at 385-88 (discussing controversy at diplomatic conference). The DMCA included a provision substantially limiting on online service provider liability. See 17 U.S.C. sec. 512.
[51] WIPO Copyright Treaty, supra note 6, Article 12. For a discussion of the history and meaning of this provision, see US Digital Agenda at WIPO, supra note 6, at 415-18.
[52] WIPO Copyright Treaty, supra note 6, Article 11. The draft treaty considered at WIPO included a provision quite similar to the anti-circumvention provision endorsed by the Clinton Administration in the White Paper which sought to outlaw technologies, the primary purpose or effect of which was to circumvent technical protection measures. The draft treaty provision, like the White Paper's proposed anti-circumvention regulation, was highly controversial within the United States and even more so at the diplomatic conference. Many delegations expressed concern about the impact of such regulations on fair uses and public domain information. As a consequence, the final treaty included only a very general norm on anti-circumvention. For a history of this provision, see US Digital Agenda at WIPO, supra note 6, at 409-15.
[53] Other factors besides uncertainties about the application of copyright law in the digital environment may be responsible for the slower-than-anticipated growth in the market for digital versions of copyrighted works. See, e.g., Pamela Samuelson, Authors' Rights in Cyberspace: Are New International Rules Needed?, First Monday (Oct. 1996), http://www.firstmonday.dk/issues/issue4/samuelson/index.html. However, there is a better case for such uncertainties being an impediment on an international scale than in the United States. That U.S. copyright law protects authors against unauthorized digital reproductions of their works has been clear since 1979. See NATIONAL COMMISSION ON NEW TECHNOLOGICAL USES OF COPYRIGHTED WORKS, FINAL REPORT (1979). In some countries, however, this was not as clear. Insofar as the WIPO Copyright Treaty clarified this on an international basis, it did contribute to the legal infrastructure for global e-commerce. See US Digital Agenda, supra note 6, at 382-85 (discussing some lack of clarity about the reproduction right in the digital environment).

commerce to flourish.[54] These norms are as "predictable, minimalist, consistent, and simple" components of a legal environment for commerce as one could expect copyright professionals to devise.[55] Thus, the WIPO treaty itself norms compatible with Framework principles and with the needs of the digital economy. That nearly one-hundred sixty nations signed this treaty indicated a strong consensus that digital works should be given appropriate protection on an international scale.[56] This was very good news for U.S. digital economy industries.

The WIPO treaty digital copyright norms were, however, mostly old news for U.S. law.[57] Its case law had already recognized the rights of authors to control digital reproductions of their works,[58] as well as to control digital transmissions of their works to the public.[59] Courts had invoked fair use in a number of digital copyright cases,[60] including one in which a copyright owner sought unsuccessfully to hold an online service provider liable for infringing acts of users.[61] Because of the substantial accord between the WIPO treaty norms and existing U.S. law, the Clinton Administration initially considered sending the WIPO Copyright Treaty to the Senate for ratification "clean" of implementing legislation.[62] This would have avoided the kind of protracted legislative battle that occurred when Congress considered the Administration's White Paper legislation in 1996.[63] Eventually, the Administration decided that implementing legislation was necessary for the U.S. to comply with the WIPO treaty provision requiring protection for the integrity of copyright management information.[64] The DMCA implementation of this norm, which closely tracks the treaty language, was uncontroversial during the legislative process.[65]

---

[54] See, e.g., E-Commerce Annual Report, supra note 4, at 13-14.
[55] Framework, supra note 1, at 3.
[56] See List of Participants, WIPO Doc. No. CRNR/DC/INF .2, Dec. 20, 1996.
[57] The WIPO Copyright Treaty, as finally concluded, was actually far more consistent with U.S. copyright law than the draft treaty with which the negotiations had begun (and which was substantially based on proposals by U.S. officials). See US Digital Agenda at WIPO, at 434-37.
[58] See, e.g., Sega Enterprises, Ltd. v. MAPHIA, 857 F. Supp. 679 (N.D. Cal. 1994).
[59] See, e.g., Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993).
[60] See, e.g., Lewis Galoob Toys, Inc. v. Nintendo of America, 964 F.2d 965 (9th Cir. 1992), cert. denied, 507 U.S. 985 (1993)(software enabling temporary changes in the play of Nintendo games held fair use).
[61] Religious Tech. Center v. Netcom On-line Comm. Corp., 907 F. Supp. 1361 (N.D. Cal. 1995).
[62] See, e.g., Clinton Administration Is Undecided On Implementing Steps For WIPO Treaties, 53 BNA Pat., Cop., & Trademark J. 241, 242 (1997).
[63] See, e.g., US Digital Agenda, supra note , at 427-32 (discussing contention over U.S. legislative proposals).
[64] See WIPO Copyright Treaty, supra note 6, Art. 12. Had this treaty defined the term "rights management information" (RMI) only as "information which identifies the work, the author of the work, the owner of any right in the work," the U.S. could have relied on Section 43(a) of the Lanham Act to assert that it was in compliance with the norms of this Article as well. See, e.g., Julie E. Cohen, Some Reflections on Copyright Management Systems, 12 BERKELEY TECH. L.J. 161, 169, n. 31. However, the treaty defines RMI as including "information about the terms and conditions of use of the work, or any numbers or codes that represent such information." Section 43(a) would not seem to cover misrepresentations of this sort. See 15 U.S.C. sec. 1125(a). See Cohen, supra, at 169, n. 31. In addition, it appears that some technical amendments to U.S. law were necessary to change the terminology about which foreign nationals could claim rights under U.S. law. See Section-by-Section Analysis of H.R. 2281 As Passed By the United States House of Representatives on August 4, 1998, 105th Cong., 2d. Session, at 3-4 (cited hereinafter as "House Manager's Report").
[65] 17 U.S.C. sec. 1202. Concerns had earlier been expressed that copyright management systems might be intrusive on privacy interests of users. See, e.g., Julie E. Cohen, The Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace, 28 CONN. L. REV. 981 (1996). In response to concerns of this sort, the legislative history of DMCA makes clear that CMI does not include digital information used to track or monitor usage of copyrighted works: "It would be inconsistent with the purpose and construction of this bill and contrary to the protection of privacy to include tracking and usage information within the definition of CMI." House Manager's Report, supra note 63, at 20.

The U.S. could have asserted that its law already complied with the WIPO treaty's anti-circumvention norm.[66] This norm was, after all, very general in character and provided treaty signatories with considerable latitude in implementation. Moreover, anti-circumvention legislation was new enough to many national intellectual property systems, and certainly to international law, to mean that there was no standard by which to judge how to instantiate the norm. The U.S. could have pointed to a number of statutes and judicial decisions that establish anti-circumvention norms.[67] With U.S. copyright industries thriving so well in the current legal environment, it would have been fair to conclude that copyright owners already had adequate protection from the law.[68] Even many of those who favor use of technical systems to protect digital copyrighted works have expressed skepticism about the need for or appropriateness of anti-circumvention regulations, at least at this stage.[69] Let content producers build their technical fences, advised one prominent information economist, but do not legislatively reinforce those fences until experience proves the existence of one or more abuses in need of a specific cure.[70] However, the political reality and legislative dynamics of the WIPO Copyright Treaty implementation process were such some sort of anti-circumvention provision appeared to be a necessary part of the bill.

Even if a rational assessment of U.S. law had led policymakers to conclude that some additional anti-circumvention legislation was necessary or desirable, one would have thought that the Administration would have supported a "predictable, minimalist, consistent, and simple" legal rule, as its Framework principles call for. The Administration might have, for example, proposed to make it illegal to circumvent a technical protection system for purposes of engaging in or enabling copyright infringement. This, after all, was the danger that was said to give rise to the call for anti-circumvention regulations in the first place. This was, in fact, the approach suppported by Silicon Valley Representative Tom Campbell in his alternative bill.[71] If this same assessment caused policymakers to decide there was a need for some regulation of circumvention technologies to promote electronic commerce, a "predictable, minimalist, consistent, and simple" legal rule would have been to outlaw making or distributing a technology intentionally designed or produced to enable copyright infringement.[72] Many "digital economy" firms and organizations supported the first of these proposals,[73] and they would likely have supported the second if it had ever had a chance of being taken seriously.

The Administration opted instead to support an unpredictable, overbroad, and maximalist set of anti-circumvention regulations. During Congressional consideration of these provisions, these regulations became complex and inconsistent for reasons that will become evident in later sections of the Article.[74] It

---

[66] See supra note --. It is far more plausible that the U.S. is in compliance with this norm than that it is in compliance with the moral rights provision of the Berne Convention, which is one of the minimum standard rules required of Berne Union members. See Berne Convention, supra note 6, Article 6bis. See Jessica Litman, The Tales That Article 2B Tells, 13 BERKELEY TECH. L.J. 931, 932 (1998)(discussing the U.S. rationale for being in compliance with the Berne Convention's moral rights provision and skepticism about the accuracy of this claim).

[67] See White Paper, supra note 14, at 232-34 (discussing statutes); Sega Enterprises, Ltd. v. MAPHIA, 857 F. Supp. 679 (N.D. Cal. 1994)(finding copyright liability for providing tools to enable game software to be removed from disks and posted on the Internet).

[68] See, e.g., White Paper, supra note 6, at 131 (reporting success of U.S. copyright industries).

[69] See, e.g., Tom W. Bell, Fair Use vs. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine, 76 N.C. L. REV. 557, 561-62 (1998); David Friedman, In Defense of Private Orderings, 13 BERKELEY TECH. L.J. 1151, 1163-64, n. 31 (1998).

[70] See, e.g., Ejan MacKaay, The Economics of Emergent Property Rights on the Internet, in THE FUTURE OF COPYRIGHT IN A DIGITAL ENVIRONMENT 21 (P. Bernt Hugenholtz, ed. 1996). "It is this restraint," says MacKaay, "that guards us from sliding into rent-seeking." Id. at 22.

[71] See H.R. 3048, 105th Cong., 1st Sess., Sec. 8.

[72] This was how most previous regulations of circumvention technologies had been framed. See, e.g., Thomas C. Vinje, A Brave New World of Technical Protection Systems, 8 EUR. INTELL. PROP. REV. 431 (1996).

[73] See supra note --.

[74] The anti-circumvention regulations are one of a number of amendments to the Copyright Act of 1976 that are contributing to its becoming increasingly unreadable. See also 17 U.S.C. sec. 104A (restoration of

was, in short, not the needs of the digital economy that drove adoption of the anti-circumvention provisions in the DMCA. Rather, what drove the debate was high rhetoric, exaggerated claims, and power politics from representatives of certain established but frightened copyright industries. These groups seem to believe they are so important to America that they should be allowed to control every facet of what Americans do with digital information.[75] They also seem to think they are entitled to control the design and manufacture of all information technologies that can process digital information.[76] The DMCA caters to their interests far more than to the interests of the innovative information technology sector or of the public.

III. DMCA'S OVERBROAD ANTI-CIRCUMVENTION PROVISIONS ARE NEITHER CONSISTENT WITH FRAMEWORK PRINCIPLES NOR GOOD FOR THE NEW ECONOMY.

There are three principal rules in the final DMCA's anti-circumvention provision. The first is section 1201(a)(1) (A) which generally outlaws the act of circumventing "a technical measure that effectively controls access to a work protected under this title."[77] This rule will, however, not take effect for two years from enactment, in part to allow time for a study to be conducted of the potential impact of this norm on noninfringing uses of copyrighted works.[78] When it does come into force, it will be subject to seven complex exceptions which will be discussed below in Section V.[79]

The other two principal rules of section 1201 are its "anti-device" provisions. Sections 1201(a)(2) and 1201(b)(1) both regulate technologies with circumvention-enabling capabilities. The former pertains to technologies that "effectively control access to [copyrighted] works,"[80] and the latter to technologies that "effectively protect[] a right of a copyright owner…in a work or a portion thereof."[81] As to each, section 1201 states that "[n]o person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof" if it has one or more of following three characteristics: (1) if it is "primarily designed or produced for the purpose of circumventing protection afforded by a technological measure" used by copyright owners to protect their works,[82] (2) if it has "only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure" used by copyright owners to protect their works,[83] or (3) if it is "marketed by that

---

copyright in foreign works that had fallen into the public domain for lack of compliance with U.S. formality rules in effect until 1989). This is not to say that the 1976 Act was a model of comprehensibility in all respects. See, e.g., 17 U.S.C. sec. 111-112 (exceptions permitting passive retransmission of broadcast signals by cable systems and ephemeral recordings during broadcast transmission). However, these incomprehensible provisions had at least been negotiated by affected industry sectors who understood what the provisions meant, even if virtually no one else could comprehend them. In contrast, the restoration of foreign copyright and anti-circumvention regulations have affect a broad range of industries. This makes more serious difficulties in comprehending the meaning of these provisions.

[75] See, e.g., Samuelson, supra note 14 (discussing the copyright maximalist agenda the Clinton Administration has supported).

[76] The potential for broad anti-circumvention regulations to give copyright owners power to control the design of consumer electronics products was recognized in Geneva. See John Browning, Africa 1, Hollywood 0, 5.03 WIRED 61, 186 (March 1997) ("Japan and other nations were up in arms about proposals that would effectively have turned the consumer electronics industry into a branch of publishing.") Indeed, some unnoticed provisions of the DMCA will require the makers of consumer videotape recorders to build in anti-copying technology in subsequent models. See 17 U.S.C. sec. 1201(k).

[77] 17 U.S.C. sec. 1201(a)(1)(A).

[78] Id. See infra notes – and accompanying text.

[79] Id. at 1201(d)-(j), discussed infra notes – and accompanying text.

[80] Id. at 1201(a)(2). See also id. at 1201(a)(3)(defining the phrases "circumvent a technical measure" and "effectively controls access to a work").

[81] Id. at 1201 (b)(1). See also id. at 1201(b)(2)(defining the terms "circumvent protection afforded by a technical measure" and "effectively protects a right of the copyright owner under this title").

[82] Id. at 1201(a)(2)(A), (b)(1)(A). There is no definition of "primarily designed or produced" in the statute; nor are any criteria for determining it provided in the statute.

[83] Id. at 1201(a)(2)(B), (b)(1)(B). This subsection may be the broadest and most dangerous of the three conditions because it would seem to put at risk "freeware" or "shareware" programs that, by their very

person or another acting on its behalf with that person's knowledge for use in circumventing technical protection afforded by a technological measure" used by copyright owners to protect their works.[84] The anti-device rules have a narrower range of exceptions.[85]

One would have to admit that the act of circumvention rule initially sought by the Administration was simpler, and at least in this respect, more consistent with the Framework's principles. It would have outlawed circumventions of technical protection systems except when done for legitimate law enforcement or intelligence purposes.[86] But this norm, in addition to violating the Framework's minimalism principle, would also have violated the Einsteinian norm to "make things as simple as possible but no simpler."[87] Representatives of major information technology firms and organizations brought to Congress's attention that this norm would interfere with many legitimate activities.[88] It would, for example, have outlawed encryption research and computer security testing, even though these activities are critical to achieving many of the objectives of the digital economy.[89] As Congress came to recognize that there were a number of legitimate reasons to circumvent technical protection systems , the bill slowly accreted exceptions that made the bill more complicated but less harmful to growth of the new economy.[90]

These same firms and organizations, in alliance with major consumer electronics firms, were also critical of the Administration's preferred anti-device provisions.[91] However, these digital economy groups spent such political capital as they had to get appropriate exceptions to the anti-circumvention norm[92] and to establish that they had no affirmative duty to build their technologies to respond to technical protection systems, but only a duty to refrain from actively undermining them.[93] They took some comfort in statements by Congressional supporters of a limited interpretation of the anti-device norms to indicate their belief that Congress meant for the anti-device provisions to apply to "'black boxes' that are expressly intended to facilitate circumvention."[94] Still, the new economy sector remains understandably concerned

---

nature, have no commercial uses. MIT Professor Hal Abelson has informed me that he expressed his reservations about this subsection to Rep. Barney Frank who serves on the House Intellectual Property Subcommittee. Prof. Abelson said that this provision should outlaw technologies having "only limited legitimate uses." He reports that Rep. Frank agreed with this assessment. Yet the final provision retains the "limited commercial purposes" construction with which it began. Email correspondence with Hal Abelson, Feb. 28, 1999.

[84] Id. at 1201(a)(2)(C), (b)(1)(C).

[85] See, e.g., id. at 1201(g)(4), (j)(4).

[86] See, e.g., Section 1201 of H.R. 2281, as introduced in the House of Representatives on July 29, 1997, reproduced in 54 BNA Pat., Trademark, & Cop. J. 270 (July 31, 1997).

[87] Albert Einstein, [source tba]

[88] See, e.g., Black Testimony, supra note 16.

[89] See, e.g., Letter from Dr. Charles Brownstein, Chair of the Public Policy Committee of the US Chapter of the Association for Computing Machinery, to Representative Thomas J. Bliley, Chairman of the House Commerce Committee, on September 29, 1998 (expressing concern about impact of broad anti-circumvention regulations on computer security research). See also Framework, supra note 1, at (emphasizing the importance of computer security to the growth of global economic commerce).

[90] See Section VI.

[91] See, e.g., Testimony of Chris Byrne, Director of Intellectual Property, Silicon Graphics, Inc., Testimony of Jonathan Callas, Chief Technology Officer, Network Associates, Inc., Testimony of Seth Greenstein, Esq., on behalf of the Digital Media Association, Testimony of Walter H. Hinton, Vice President, Storage Technology Corp., on behalf of the Computer and Communication Assocation, Testimony of Gary J. Shapiro, Chairman of the Home Recording Rights Coalition and President of Consumer Electronics Manufacturers' Association, House Commerce Hearing, supra note --.

[92] See 17 U.S.C. sec. 1201(f), (g), and (j).

[93] 17 U.S.C. sec. 1201(c)(3). See Statement of Congressman Bliley, CONG. REC. H7095 (8/4/98).

[94] See id. at H7094-95. See also House Manager's Report, supra note --, at 9 ("[Section 1201(a)(2)] is carefully drafted to target 'black boxes' and to ensure that legitimate multipurpose devices can continue to be made and sold.")

about the potential for overbroad application of the anti-circumvention and anti-device norms, and recent developments suggest that there is reason for this concern.[95]

Although Administration officials admitted in Congressional testimony that its preferred legislation went beyond what the WIPO Copyright Treaty required, it argued for this broader rule in part to set a standard that would help the U.S. persuade other countries to pass similarly strong rules. [96] Proponents of the Administration's preferred anti-circumvention regulations scoffed at arguments made by an alliance of consumer electronics firms and by representatives of computer and software industry about the mischief that broad anti-circumvention regulations would do in this industry.[97] They also dismissed as specious arguments made by library and educational groups about threats to fair use and the public domain arising from broad anti-circumvention regulations.[98]

IV. THE LIST OF EXCEPTIONS IN THE ACT OF CIRCUMVENTION BAN IS UNDULY NARROW AND INCONSISTENT WITH FRAMEWORK PRINCIPLES.

The DMCA ban on the act of circumvention of technical protection systems is subject to seven very specific exceptions,[99] as well as being qualified by several other subsections.[100] In addition, it is subject to a two-year moratorium during which the Librarian of Congress is supposed to study the potential impact of the anti-circumvention ban on noninfringing uses of copyrighted works which may lead to further limitations on the act of circumvention rule.[101] While several of these exceptions and limitations respond to the gravest of concerns expressed by digital economy firms,[102] they are still too narrowly crafted, as examples given below will reveal.[103] Congress should have adopted a provision enabling courts to exempt acts of circumvention engaged in for other legitimate purposes. Courts interpreting section 1201 may either be forced to find liability in some situations in which it would be inappropriate to impose such liability or to stretch existing limitations. Congress may eventually need to revise this provision to recognize a broader range of exceptions.

The structure of the final DMCA anti-circumvention provisions and its complexity can be explained resulting from the maximalist position with which the Administration and their major copyright industry allies began the legislative struggle. Only when industry groups were able to identify particularized situations in which circumvention was appropriate was there any legislative "give" on the issue, and then only to the extent of that identified situation.[104] As noted above, the Administration initially sought to an almost unlimited ban of circumvention activities. The only exception to anti-circumvention ban in the Administration's favored legislation was that which would enable circumvention of technical protection systems for legitimate law enforcement, intelligence, and other governmental purposes. [105] Without this exception, suspected Mafia bosses and terrorists, oddly enough, might have been able to

---

[95] See infra notes – and accompanying text.
[96] See, e.g., House Subcommittee Holds Hearings on WIPO Treaty Bills, OSP Liability, 54 BNA Pat., Trademark, & Cop. J. 414 (9/18/97).
[97] See, e.g., Testimony of Allan Adler, House Jud. Hearing, supra note 16.
[98] See, e.g., Testimony of Michael Kirk, House Jud. Hearing, supra note 16.
[99] 17 U.S.C. sec. 1201(d)-(i).
[100] Id. at sec. 1201(c)(1)-(4).
[101] Id. at 1201(a)(1)(A)-(C).
[102] Id. at 1201(f) (reverse engineering exception), (g)(encryption research), and (i)(computer security testing). See, e.g., Black Testimony, supra note 16 (expressing concern about reverse engineering); Callas Testimony, supra note – (expressing concern about encryption and security research).
[103] See infra notes – and accompanying text.
[104] See supra note --.
[105] See Section 1201(e) of H.R. 2281, as introduced in the House of Representatives on July 29, 1997. The DMCA version of 1201 has such a provision, although it has been expanded to enable government agencies to test the vulnerabilities of their computer systems or networks. See 17 U.S.C. sec. 1201(e).

challenge attempted law enforcement or intelligence agency decryptions of their records or communications under Section 1201(a)(1).[106]

The Administration's preferred bill also provided that nothing in Section 1201 would "affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title."[107] This seemed to recognize that circumventing a technical protection system for purposes of engaging in fair use or other noninfringing acts would be lawful, although it does not directly say so.[108] However, some representatives of major copyright industries who testified at a Congressional hearing on this legislation expressed the view that fair use should not be an acceptable reason to "break" a technical protection system used by copyright owners to protect their works.[109] Allan Adler, testifying on behalf of the Association of American Publishers, for example, stated that "the fair use doctrine has never given anyone a right to break other laws for the stated purpose of exercising the fair use privilege. Fair use doesn't allow you to break into a locked library in order to make 'fair use' copies of the books in it, or steal newspapers from a vending machine in order to copy articles and share them with a friend."[110] The "breaking and entering" metaphor for circumvention activities swayed some influential Congressmen in the debate over anti-circumvention regulations.[111]

Courts may eventually distinguish between circumvention aimed at getting unauthorized access to a work and circumvention aimed at making noninfringing uses of a lawfully obtained copy.[112] Section 1201(a)(1) is more clearly aimed at the former than at the latter. Fair use, for example, would provide a poor excuse for breaking into a computer system in order to get access to a work one wished to parody. However, if one had already lawfully acquired a copy of the work, and it was necessary to bypass a technical protection system to make fair use from that copy, this would arguably be lawful under Section 1201(a)(1) and (c)(1).[113] Take, for example, an act of circumvention performed by a friend of mine who works for Xerox's Palo Alto Research Center. He is an expert witness in a lawsuit challenging the Washington Redskins' trademark on the ground that the word "redskins" is scandalous or disparaging.[114] This researcher decided it was necessary to take a clip from an old Western movie to demonstrate derogatory uses of the term in context. It was necessary for him to defeat a technical protection system adopted by the owner of the copyright in this movie in order to make the clip for this purpose. The

---

[106] Virtually all such records would likely embody a modicum of originality that would enable these actors to claim copyright protection in fixations of these records. If these persons used technical protection systems to prevent unauthorized access to these records, any act of the government to circumvent such systems would, strictly speaking, run afoul of Section 1201(a)(1).

[107] Section 1201(d) of H.R. 2281, as introduced in July 1997. See 17 U.S.C. sec. 1201(c)(1).

[108] An extremely narrow interpretation of the provision might suggest that fair use could be raised as a defense to an infringement claim based on activities engaged in after a circumvention had taken place (e.g., reproducing a portion of the work for fair use purposes), even if the act of circumvention itself would not be excused. See, e.g., Testimony of Michael Kirk, House Jud. Hearing, supra note 16.

[109] See also White Paper, supra note 14, at 231 (indicating that copyright owners have no obligation to make their works available in a form that will enable fair uses to be made of them).

[110] Adler Testimony, supra note 18, at [6]. This same speaker went on to say that "[t]he Declaration of Independence is in the public domain, but there is nothing wrong with the National Archives keeping it in a vault and punishing anyone who tries to break through security to get hold of that copy." Id.

[111] See, e.g., House Manager's Report, supra note --, at 5 (charcterizing circumvention to get unauthorized access "is the electronic equivalent to breaking into a locked room to obtain a copy of a book"). But see, e.g., Friedman, supra note --, at 1163, n. 31 (arguing against the treatment of technologies capable of circumventing technical protection systems as "the digital equivalent of burglar's tools").

[112] See, e.g., Cohen, supra note 63, at 174-76 (discussing lawful circumventions). See also Julie E. Cohen, Copyright and The Jurisprudence of Self-Help, 13 BERKELEY TECH. L.J. 1089 (1998)(finding in copyright's fair use doctrine an affirmative right to "hack" technical protection systems to make fair uses).

[113] See, e.g., Letter from Rep. Howard Coble to Rep. Rick Boucher, introduced into the Congressional Record during the debate leading to passage of H.R. 2281 in the House of Representatives, CONG. REC. H7097 (indicating an intent to distinguish between circumvention to get unauthorized access to a work and circumvention to make fair uses).

[114] See 15 U.S.C. sec. 1052(a)(excluding scandalous and disparaging matter from trademark protection).

copyright owner might argue that this technical protection system aimed to provide a limited degree of access to the movie and that the researcher's circumvention defeated an intended access control system. However, if Section 1201(c)(1)'s preservation of fair use and other defenses to infringement are to be given their plain meaning, it would seem that this sort of circumvention should be permissible.[115] Thus, if the clip from the movie qualifies as a fair use, the act of circumvention may be privileged under Section 1201(c)(1).[116]

Although this section's apparent preservation of fair use was important, it did not satisfy library and nonprofit groups who expressed substantial concern about the impact that the anti-circumvention provisions would have on public access to information.[117] The only additional concession that the House Subcommittee on Intellectual Property thought should be made to concerns expressed by these groups was to create a special "shopping privilege" for them. This exception, which was included in the final DMCA, enables nonprofit library and educational institutions to circumvent technical protection systems to "make a good faith determination of whether to acquire a copy" of the work.[118] Librarians and educators do not see much value in this provision given that vendors of technically protected copyrighted works would generally have incentives to allow librarians and educators to have sufficient access to make acquisition decisions.[119] Their broader concerns about the impact of anti-circumvention regulations on noninfringing uses fell on deaf ears in both the House and Senate Subcommittees on Intellectual Property.[120]

The initial efforts of computer and software industry groups to get additional exceptions to the anti-circumvention rules and other changes to the anti-circumvention regulations to make them less harmful to legitimate activities in these industries were also unsuccessful. [121] Not until the full Senate Judiciary Committee and the House Commerce Committee undertook their reviews of the legislation were the concerns of these industry groups heeded. Out of the Senate Committee emerged three significant changes to the DMCA. The first was creation of a new exception to enable circumvention of technical protection systems for purposes of enabling a software developer to achieve interoperability among computer programs.[122] The second was a provision clarifying that equipment manufacturers were under no obligation to specially design their products to respond to any particular technical measure used by those providing content for this equipment.[123] The third was a provision indicating that Section 1201 was not intended to broaden contributory or vicarious copyright liability.[124]

An interesting twist in the saga leading up to adoption of the DMCA was the House Commerce Committee's decision to exercise jurisdiction over part of the digital copyright legislation.[125] Its review led to several other significant changes to the bill. Some of these responded to concerns expressed by digital economy firms; others responded to concerns expressed by library, educational, and other nonprofit

---

[115] See, e.g., Statement of Representative Bliley, Congressional Record, H-7093, 8/4/98 (indicating that the Commerce Committee understood the legislation to enable consumers to "exercise their historical fair use rights"). See also Coble Letter, supra note --.

[116] But see infra notes – and accompanying text for a discussion about whether this person's development of a technology enabling him to defeat the technical protection system would be similarly privileged.

[117] See, e.g., Testimony of Robert Oakley, House Commerce Hearing, supra note --, at 64-66.

[118] See 17 U.S.C. sec. 1201(d).

[119] See infra notes – and accompanying text concerning whether the shopping privilege could be undermined by the lack of available tools to enable this circumvention.

[120] See, e.g., Testimony of Robert Oakley and Testimony of M.R.C. Greenwood, House Jud. Hearing, supra note – (expressing concerns about the impact of technical protection systems on noninfringing uses of protected works). The "shopping privilege" does not address these concerns.

[121] See, e.g., Black Testimony, supra note 16 (expressing concern about the impact of the anti-circumvention provisions for achieving interoperability among computer programs).

[122] See 17 U.S.C. sec. 1201(f).

[123] Id. at sec. 1201(c)(3).

[124] Id. at sec. 1201(c)(2).

[125] See, e.g., Statement of Rep. Tauzin, House Commerce Hearing, supra note --, at 2-3 (explaining the Commerce Committee's reasons for reviewing the WIPO treaty implementation legislation).

groups.[126] The Commerce version of the bill added a new exception to enable encryption research and the development of encryption-research tools.[127] It also created two consumer-oriented exceptions, one to enable parents protect their children from accessing material on the Internet, and the other to enable circumvention to protect personal privacy.[128] It also proposed a moratorium on the anti-circumvention rules so that a study could be conducted about the potential impact of anti-circumvention rules on fair use, the public domain, and other noninfringing uses of copyrighted works.[129]

More clearly than the Judiciary Committees in either branch of Congress, the Commerce Committee recognized the unprecedented nature of the access right that was implicit in the act of circumvention provision of Section 1201. "If left unqualified," said Congressman Bliley, "this new right…could well prove to be the legal foundation for a society in which information becomes available only on a 'pay-per-use' basis."[130] To ensure this would not occur, the legislation was amended to enable librarians and educators to make a showing that the anti-circumvention provision was interfering with noninfringing uses of copyrighted materials and to seek an exemption from the ban.[131] Insofar as such a showing could be made, the Commerce Committee thought that affected classes of works or of users should be exempt from Section 1201(a)(1)(A). Congressman Bliley pointed out that "[c]opyright law is not just about protecting information. It's just as much about affording reasonable access to it as a means of keeping our democracy healthy."[132] The Commerce Committee review of the legislation also led to inclusion of a provision indicating that nothing in Section 1201 "shall enlarge or diminish any rights of free speech or of the press for activities using consumer electronics, telecommunications, or computing products."[133] This provision recognizes the potential impact of the anti-circumvention rule on free speech and free press interests.

During the final negotiations leading up to passage of the DMCA, several of the exceptions were refined.[134] In addition, the computer security research community finally persuaded legislators to add another exception to enable circumvention of technical protection systems necessary for legitimate testing of the security of computer systems.[135]

While the final version of the DMCA anti-circumvention provision responded to several significant concerns of the digital economy sector, it did so mainly by adopting specific exceptions. There are, however, many other legitimate reasons for circumventing technical protection systems that are not, strictly speaking, covered by the exceptions in the final bill. Five examples will be cited to demonstrate that Section 1201 should have a "or other legitimate purposes" exception to Section 1201(a)(1).

Suppose, for example, that a copyright owner had reason to believe that an encrypted work contained an infringing version of one of its works. The only way to find out whether the copyright owner's suspicion is valid may be to circumvent the technical protection system to get access to the encrypted material. Even if its suspicions proved correct, the copyright owner would have violated section 1201(a)(1)(A) in the course of discovering this. There is no exception in section 1201 to privilege this kind of decryption activity.

Or suppose that a content producer had licensed certain software that was essential to the development of its product (e.g., editing software used in the process of making motion pictures). In the

---

[126] See, e.g., Commerce Panel Clears Digital Copyright Bill With Further Concessions on Fair Use, 56 BNA Pat., Trademark, & Cop. J. 326 (7/23/98).
[127] This eventually was codified in the DMCA. See 17 U.S.C. sec. 1201(g).
[128] These were also eventually codified in the DMCA. See id. at sec. 1201(h),(i).
[129] Id. at sec. 1201(a)(1)(B). See infra notes – and accompanying text for discussion of this provision.
[130] Bliley Statement, supra note --, at H7094.
[131] 17 U.S.C. sec. 1201(a)(1)(B)-(D). See infra notes – and accompanying text.
[132] Bliley Statement, supra note --, at H7094-95.
[133] See 17 U.S.C. sec. 1201(c)(4).
[134] Compare H.R. 2281 as passed on Aug. 4, 1998, with Pub. L. No. 105-304.
[135] 17 U.S.C. sec. 1201(j). This too had been the subject of testimony before the House Commerce Committee. See, e.g., Callas Testimony, supra note --.

course of a dispute about the performance quality of this software, the content producer might withhold payment of a royalty as a way of communicating its displeasure with the licensor's maintenance of the software. The software's licensor might then respond by activating a technical "self-help" system embedded in the software to stop its operation.[136] To deal with this development, the licensee might well attempt to circumvent the self-help feature blocking access to the software because the licensee needed to use the software to finish its movie and because it regarded itself as having a legitimate claim of breach by the licensor which justified holding back the royalty.[137] However legitimate the claim or this activity, there is no exception to the anti-circumvention rule to protect the licensee in this situation.

A third and fourth examples will illustrate the narrowness of certain existing privileges in the DMCA. Suppose, for example, that a firm circumvented a technical protection system to stop software it had licensed from monitoring certain uses of the software in ways not contemplated in the license agreement and which the licensee regarded as unwarranted and detrimental to its interests. Although there is a "personal privacy" exception in the DMCA,[138] there is no general exception for circumventing to protect appropriate confidentiality interests. Or suppose that a firm was considering making a multi-million dollar acquisition of a computer system whose producer asserted was highly secure. If this firm wished to test the veracity of the producer's assertions, either without getting the producer's permission or over the producer's objection, it would seem to violate Section 1201. Although there is a computer security testing exception in the Act, it only applies if one is already the owner or operator of the computer system being tested.[139] It should be noted here that many security flaws discovered in widely deployed systems have been found by researchers who tested the system without permission of either the owner or manufacturer of such systems.[140] These activities too are not covered by the computer security exception provided for in the DMCA.

Finally, since the DMCA recognizes that the anti-circumvention rules may have an impact on free speech and free press concerns,[141] it may be worth considering an example of this sort. Suppose that an employee of a major chemical company gave a reporter a disk containing a digital copy of a report and several photographs pertaining to a major chemical spill that the company was trying to cover up. If information on the disk was technically protected and the employee was not authorized by the company to provide the information to the reporter, it would appear that the reporter would violate Section 1201(a) if he circumvented the technical protection system to get access to this information, even if consideration of free press and free speech interests might suggest that such a circumvention was justifiable.

---

[136] Software developers can embed specialized disabling subprograms in licensed software. These may operate so that the software ceases operation unless a new code has been made available to the licensee by the licensor. They can also be invoked via a network connection to the licensor's site or by a remote act by the licensor. For a discussion of public policy issues raised by technical self-help systems, see, e.g., Pamela Samuelson, Embedding Technical Self-Help in Licensed Software, 40 Comm. ACM 13 (Oct. 1997).

[137] A model law to regulate licensing of computer information has proposed to validate, as a matter of contract law, a licensor's use of technical self-help systems as long as certain procedural steps are taken to protect licensee intersts. See Article 2B of the Uniform Commercial Code, Sec. 2B-716, as of February 1999. See, e.g., Memorandum of Susan H. Nycum to Uniform Commercial Code Article 2B Reporter and Drafting Committee regarding Licensor Self-Help Revision of Proposed UCC2B, Jan. 27, 1997, at 1 (expressing objections to proposed validation of technical self-help features in licensed software, speaking of them as a "trap for the unwary—in the extreme"). See also Memorandum from Michele Kane on behalf of Walt Disney Co. to Prof. Raymond T. Nimmer, Reporter for Article 2B, dated Jan. 27, 1997, at 3 (strenuously objecting to Article 2B's endorsement of technical self-help provisions in model licensing law as "unnecessary and unfair").

[138] 17 U.S.C. sec. 1201(i). For a discussion of the concerns leading to adoption of this exception, see Testimony of Marc Rotenberg, House Commerce Hearing, supra note --.

[139] 17 U.S.C. sec. 1201(j).

[140] See, e.g., [NY Times article about Berkeley student Ian Goldberg discovering a flaw in Netscape's Secure Socket Layer].

[141] 17 U.S.C. sec. 1201(c)(4).

One response to these examples might be to assert that copyright owners will generally not sue when these or other legitimate circumvention activities occur. However, in some of the examples given above, the technical protector might well have incentives to sue the circumventor.[142] Given that there are serious criminal penalties for willfully violating Section 1201,[143] the overbreadth of this provision and the narrowness of existing exceptions will put many legitimate circumventors at unnecessary risk. If such suits are brought, courts may, of course, and probably will, find other ways to reach just results. They might, for example, decide that the "other defenses" provision of the anti-circumvention rule legitimized the circumvention,[144] that some instances were within the spirit, even if not the letter, of an existing privilege, or that there was insufficient harm to the legitimate interests of the person challenging the circumvention activity to justify imposing liability.[145] However, there should be a general purpose "or other legitimate purposes" provision in Section 1201 so that courts will not have to thrash to reach appropriate results. This would add flexibility, adaptability, and fairness to the law. In many other parts of copyright law—with the fair use doctrine, for example, or the distinction between ideas and expressions—Congress has trusted the common law process to distinguish between legitimate and illegitimate activities. It could (and should) have done so with respect to circumvention legislation as well.

It would have been especially appropriate to adopt a general purpose "other legitimate purpose" provision because the anti-circumvention ban is an unprecedented provision for copyright law as to a significant new technology issue with which neither Congress nor the courts have much experience.[146] The lack of a general purpose exception is particularly troubling in view of the harsh criminal and civil provisions in the statute, which may have a chilling effect on legitimate activities, including those affecting free speech. It could also put at risk some legitimate activities in the digital economy that will impede the growth of e-commerce, as will become more apparent in the next subsection.

V. THE ANTI-DEVICE PROVISIONS SHOULD BE NARROWED BY LEGISLATIVE AMENDMENT OR JUDICIAL INTERPRETATION.

The text of the DMCA and in its legislative history clearly demonstrates that Congress intended to ensure that users would continue to enjoy a wide range of noninfringing uses of copyrighted works, even if copyright owners used technical protection systems to impede them. This is evident in the DMCA's seeming recognition that circumventions for fair use, free speech, and free press purposes should be lawful.[147] It is also apparent in the provision enabling the Librarian of Congress to exempt certain classes of users or works from the general anti-circumvention ban when necessary to preserve socially valued noninfringing uses.[148] In addition, it explains why Congress adopted some exceptions to the act of circumvention ban, notably, the interoperability privilege.[149] As the last section has shown, if Congress had

---

[142] See supra note – (licensor whose self-help feature might be defeated by a licensee).
[143] 17 U.S.C. sec. 1204.
[144] 17 U.S.C. sec. 1201(c)(1).
[145] 17 U.S.C. sec. 1203(a) requires that a person be "injured by a violation of section 1201" in order to bring a suit to challenge a violation of this provision.
[146] Professor Julie Cohen, in commenting on the structure of Section 1201, observed that this provision is almost European in its construction. Typically, European legislators formulate laws as though all contingencies can be foreseen and the rule can be established for all time. Europeans typically provide a broad rule and only limited exceptions to the rule. American laws more typically have some openness that allow the laws to adapt to new circumstances. This may provide American law with needed flexibility in times of rapid technological change. Yet, Section 1201 deviates from this general American approach. Communication with Julie E. Cohen, Jan. 1999.
[147] Id. at 1201(c)(1), (c)(4), discussed supra notes – and accompanying text. This same subsection indicates that it also does not intend to enlarge or diminish vicarious or contributory copyright infringement. Id. at 1201(c)(2).
[148] Id. at 1201(a)(1)(B)-(D).
[149] Id. at 1201 (f). This exception preserves the fair use privilege recognized in Sega Enterprises, Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992) that permits the intermediate copying of computer programs when necessary to obtain information in order to achieve interoperability among independently developed computer programs.

not been blinded by the politics of the day, it would likely have recognized other legitimate reasons to engage in acts of circumvention.

If Congress intended for circumvention of technical protection systems to be legal when done for legitimate purposes, it might seem obvious that Congress should be understood to have intended to enable users to effectuate the circumvention privileges it recognized.[150] Although it will not always be necessary for a legitimate circumventor to make or use a circumvention technology to accomplish a privileged circumvention (e.g., a print enciphered text can be broken by purely mental activity), most often this will be necessary.[151] The deepest puzzle of Section 1201 is whether Congress implicitly intended to allow the development and/or distribution of technologies necessary to accomplish legitimate circumvention activities, or whether, in essence, it created a number of meaningless privileges.

Seemingly relevant to addressing this question are some curious features of Section 1201 that close study of this complex provision reveals. First, it is noteworthy that several exceptions to the anti-circumvention rule specifically authorize the creation of tools necessary to achieving a legitimate circumvention activity (e.g., the encryption research and interoperability privileges),[152] while several others (e.g., the law enforcement privilege and the privacy privilege) do not.[153] Secondly, while the interoperability privilege exempts necessary tools from both device provisions of Section 1201,[154] the encryption and security research privileges exempt tools only from the access-device provision, not from the control-device provision. Yet, it would seem that encryption and security research would often require testing both of access and of control components of technical protection systems.[155] Thirdly, Section 1201 contains no provision enabling the development or distribution of circumvention tools to enable fair use or other privileged uses in terrain which Section 1201(a)(1)(A) arguably doesn't reach (i.e., making fair uses of lawfully acquired copies). If Congress intended to recognize a right to "hack" a technical protection system to make fair uses, this right could be undermined if it could not be exercised without developing a tool to bypass the technical protection system or otherwise getting access to such a tool.[156] Under some interpretations of Section 1201(b)(1), development or distribution of such a tool would be unlawful.

Consider, for example, the Xerox PARC researcher who circumvented a movie's technical protection system in order to make a fair use clip for the Washington Redskins' litigation.[157] It was necessary for him to develop a tool to enable him to bypass the technical protection system to make the clip. Suppose that the motion picture copyright owner found out about the circumvention and decided to make an example of this researcher, suing him for $25,000 in statutory damages for violating Section 1201(b)(1).[158] On a strict interpretation of this subsection, the researcher might seem to be in trouble. The

---

[150] See, e.g., Benkler, supra note --, at [81] ("If the act of circumvention were privileged to users, particularly if it were privileged as a matter of free speech, it would be difficult to sustain a prohibition on manufacture and sale of the products necessary to enable them to engage in circumvention.").

[151] See, e.g., James R. Davis, On Self-Enforcing Contracts, the Right to Hack, and Willfully Ignorant Agents, 13 BERKELEY TECH. L.J. 1145, 1147 (1998)(questioning whether a "right to hack" to make fair uses would be meaningful given that most people would not be able to do so without tools to enable this).

[152] See 17 U.S.C. sec. 1201(f),(g).

[153] See 27 U.S.C. sec. 1201(e)(i). There is, however, a better textual argument for inferring a tool-making privilege for law enforcement activities than for inferring tool-making authority to enable privacy protection. Section 1201(i) limits the application of Section 1201(a)(1)(A), whereas Section 1201(e) indicates that "this section does not prohibit any lawfully authorized investigative…activity" of a government agent.

[154] Id. at 1201(f)(2).

[155] Id. at 1201(g)(4), (j)(4).

[156] See also Cohen, supra note 63, at 174-78 (discussing legal tampering with technical protection systems and its implications for the availability of tools to accomplish this).

[157] See supra note – and accompanying text.

[158] See 17 U.S.C. sec. 1203(c)(3). This researcher would likely be spared from criminal liability for violation of Section 1201(b) because he was serving as a pro bono publico expert witness in this case. 17 U.S.C. sec. 1204(a) requires that a violation of sec. 1201 not only be willful, but done for commercial advantage or private financial gain for criminal liability to be imposed.

tool was, after all, "primarily designed...for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of the copyright owner under this title in a work or a portion thereof." However, one can easily imagine a court deciding that the researcher's code did not run afoul of Section 1201(b)(1). The code might be viewed as a special purpose tool made for the limited purpose of effectuating fair use rights. In view of its lack of commercial significance and the absence of deleterious effects of the sort that the anti-device provisions were intended to reach,[159] a court might decide this code should not be considered a violation of this law.[160]

Would the result be different if the researcher asked a co-worker or a friend to develop the tool instead of doing it himself? Or would the result be different if the researcher shared this tool with a co-worker who needed to make a fair use circumvention of a different movie? Even though he might be "provid[ing]" this technology to another person, perhaps he would escape liability because he was not "traffic[ing]" in this technology or "offer[ing it] for sale" which are the principal activities Congress meant to curb by enacting this part of DMCA.[161] However, it is fair to observe that courts would have to read some limiting language into Section 1201(b)(1) to decide that the researcher would not be liable in all three situations.

An undoubtedly closer question is what courts would do about a technology distributed in the mass-market for purposes of enabling privileged circumventions. Consider, for example, how the *Vault v. Quaid* case would fare under the DMCA anti-device provisions.[162] Vault sued Quaid for contributory copyright infringement because Quaid developed and sold a program called Ramkey that Quaid's customers could use to defeat Vault's Prolok copy-protection software (which Vault sold to other software developers who used it to protect their software from unauthorized copying). By spoofing Vault's copy-protect system,[163] Quaid's customers could make unauthorized copies of the third-party software protected by Vault's program.[164] Quaid successfully defended against the contributory infringement claim by showing that Ramkey had a substantial noninfringing use, namely, to enable users to effectuate their rights under copyright law to make backup copies.[165]

Quaid would probably not run afoul of the access-device provision of Section 1201(a)(2).[166] However, less clear is whether it could successfully defend against a Section 1201(b)(1) claim. Suppose that Quaid's president testified that his primary purpose in designing and producing Ramkey was to enable his customers to do legitimate backup copying. Suppose further that the marketing literature for Ramkey emphasized this purpose of the program and even warned potential customers not to use Ramkey to make infringing copies. If a court considered this evidence credible, it would probably save Quaid from criminal prosecution for violating the second anti-device norm. But would it save him from civil liability? [167]

---

[159] See House Manager's Report, supra note --, at 9-13.
[160] Alternatively, the court could find only a technical or de minimis violation of the statute in this instance.
[161] 17 U.S.C. sec. 1201(b)(1).
[162] 775 F.2d 638 (5th Cir. 1985).
[163] In essence, this and other "spoofing" software generally operate by emitting a signal which will be read by he other firm's copy-protection software (or conceivably hardware) as an indication that the system is operating effectively.
[164] Vault also claimed direct copyright infringement, trade secret misappropriation, and breach of contract. *Vault*, 847 F.2d at 257-58.
[165] See id. at xx (relying on the Supreme Court's decision in Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984) which rejected a claim that Sony had contributorily infringed Universal's movie copyrights by selling Betamax machines which enabled home copying of these movies off the broadcast television because of noninfringing uses of the Betamax machine).
[166] Quaid could probably argue that Ramkey was primarily designed to enable bypassing of the Prolok system for lawfully acquired copies of protected programs. This would seem to make section 1201(a)(2) inapplicable to the *Vault v. Quaid*-like controversies.
[167] An interesting question is who could sue Quaid under Section 1201(b)(1). The Clinton Administration's Green Paper on IP and the NII suggested that the maker of a protective technology, such as Vault, would not have standing to challenge the maker of circumvention technologies. See REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY, GREEN PAPER ON INTELLECTUAL

To answer that question, courts would have to grapple with a seeming inconsistency in the statute. On the one hand, the DMCA seems to outlaw technologies if their primary purpose is to circumvent a technical protection measure that effectively protects a right of a copyright owner to control its work (in this case, a right to control illegal copying).[168] On the other hand, the DMCA recognizes that fair use-like circumventions should be lawful.[169] Backup copying is a specially privileged activity in the copyright statute.[170] Since the copyright owner doesn't have a statutory right to control backup copying, perhaps a spoofing technology intended to enable backup copying should be outside the statute. It is important to understand that circumvention for backup copying purposes cannot occur without access to such a technology.

So if most lawful users of Prolok-protected software lack the skills to write a Ramkey-equivalent, perhaps it should be lawful to make and distribute a technology to effectuate the backup copy privilege. It is unclear whether Congress intended for the technologically savvy who could "do it themselves" to be the only ones who could engage in privileged acts of circumvention. Yet, as the example of the Xerox researcher illustrates, even they would need to develop special purpose tools to enable this which would run some risk of being held liable of a violation of Section 1201(b)(1).[171] Potentially relevant to whether the distribution of a tool like Ramkey is lawful is Section 1201 (c)(2) which states that nothing in Section 1201 "shall enlarge or diminish vicarious or contributory liability for copyright infringement in connection with any technology, product, service, device, component, or part thereof."[172] If this is true, perhaps the result in *Vault v. Quaid* would be the same after DMCA as before. One can imagine some courts deciding to construe section 1201(b)(1) narrowly so that the honest maker of a Ramkey-equivalent for purposes of enabling backup copying would be able to do so. But it is far from clear that they would do so.

Moreover, the major copyright industries that supported a broad ban on circumvention technologies would assert that courts should not do so. They would likely consider Quaid's argument that Ramkey was primarily designed and produced to enable lawful backup copying as a ruse. Moreover, they would likely point out that Ramkey doesn't just enable lawful backup copying; it enables illegal copying as well. They would regard the danger that Ramkey would be used for illegal purposes—regardless of Quaid's intent—as so substantial as to justify banning this technology. The DMCA's anti-device provisions were broadly drafted, they would argue, to address this very danger.[173] They would also consider it an unnecessary burden for copyright owners to have to prove that the primary use of a technology like Ramkey was to engage in infringement.[174] This would be difficult to do, especially for a technology that was about to be introduced into the market. When the dangers of infringement are high, they would argue, the technology ought to be deemed illegal if its purpose is to circumvent a technical protection system

---

PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 130 (July 1994). Copyright owners who used technical protection systems to protect their works would seem to have standing to initiate the suit. This could mean that a firm such as Quaid would thus be faced, not just with one lawsuit, but potentially thousands to defend. As will be discussed further infra notes – and accompanying text, in none of these lawsuits would the plaintiff have to demonstrate that any underlying acts of infringement actually took place. The White Paper was silent on the issue of standing. Nor is the issue expressly dealt with in the DMCA. Proposals by representatives of Macrovision Corp., which makes technical protection systems, to change 17 U.S.C. sec. 1203(a) to facilitate its ability to obtain standing in such a suit were not heeded by Congress. See Testimony of Mark S. Belinksy on behalf of Macrovision Corp., House Jud. Hearing, supra note 16.

[168] See 17 U.S.C. sec. 1201(a)(2), (b)(1).

[169] Id. at sec. 1201(c)(1), discussed supra notes – and accompanying text.

[170] 17 U.S.C. sec. 117.

[171] Even they, of course, may have to manufacture a technology or provide a service to make backup copies. See Benkler, supra note --, at [81].

[172] 17 U.S.C. sec. 1201(c)(3). Recall that the main claim made by Vault against Quaid was a contributory infringement claim, and it was unsuccessful. See supra note – and accompanying text.

[173] See, e.g., Testimony of Bruce Lehman, House Jud. Hearing, supra note 16.

[174] See, e.g., Valenti Testimony, supra note --.

copyright owners are using to protect rights granted to them by copyright law.[175] Under this view, Ramkey is illegal under the DMCA. The major copyright industry supporters of the broad anti-device provisions of the DMCA would probably like nothing better than to make Congress' apparent preservation of noninfringing uses into a meaningless promise.

Different judges might reach different conclusions on a Ramkey-like case, but consider how they might deal with another plausible "spoofing" technology. Intel has recently developed a line of semiconductor chips with a built-in identification system for each processor.[176] Privacy advocates have raised concerns about the threat that processor identification systems poses for personal privacy on the Internet.[177] In response to these concerns, Intel announced its intent to ship these chips with the processor identity function "off."[178] Suppose, however, that Microsoft develops Windows 2000 as a "trusted system" technology[179] to run on this line of Intel chips and that it requires that licensees of Windows 2000 agree to keep the Intel identification system on at all times.[180] Having the identifier on, Microsoft might well contend, is a critical component to the effectiveness of its trusted system technology. Suppose further that Windows 2000 will not install until the Intel identifier is on, and that the installation software, after a user clicks "I agree" to the conditions of the license, will actually turn the identifier on if necessary.[181] If privacy advocacy group developed and distributed software that would spoof Windows into thinking the Intel identifier was on when it was not in order to protect user privacy, or if the group posted information about how users could turn the identifier off even when using Windows 2000, would it be violating Section 1201(b)(1)?[182]

---

[175] There is no "authority of law" exception in the DMCA's anti-device provisions, as there was in the White Paper's original proposal for an anti-device regulation. See White Paper, supra note 14, Appendix 1 at 6. How, if at all, this might affect the scope of the DMCA's anti-device provisions remains to be seen.

[176] See, e.g., Peter H. Lewis, Whosh! The Next Pentium Chip Is On Its Way, New York Times, Jan. 14, 1999, http://www.nytimes.com/library/tech/99/01/circuits/articles/12pete.html (visited on Jan. 28, 1999).

[177] See, e.g., Jeri Clausing, Privacy Groups Seek Recall of Intel Chip, New York Times, Jan. 29, 1999, http://www.nytimes.com/library/tech/99/01/cyber/articles/29privacy.html (visited on Jan. 29, 1999). Although the threat the Intel processor ID poses for privacy has gotten the most attention in the press, the potential for the Intel processor ID to be used to prevent "piracy" of software has also been recognized. See, e.g., Peter Wayner, Debate on Intel Chip Misses Piracy Issue, http://www.nytimes.com/library/tech/99/01/cyber/articles/30chip.html (visited 2/1/99).

[178] See, e.g., Jeri Clausing, Intel Alters Chip After Boycott Threat, New York Times, Jan. 25, 1999, http://www.nytimes.com/search/daily/b…te+site=56415)2+wAAA+%22pentium%7EII%22.

[179] See, e.g., Mark Stefik, Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us To Rethink Digital Publishing, 12 BERKELEY TECH. L.J. 137 (1997) (discussing the concept of trusted system technology).

[180] This is no mere conjecture. Microsoft is reportedly intending to deploy trusted system software with the next version of Windows. See, e.g., Jason Chicola, et al., Digital Rights Architectures for Intellectual Property Protection, paper prepared for Ethics and Law on the Electronic Frontier, Fall 1998, at 38. This is especially worrisome since Microsoft has a monopoly position in the market for operating systems software, making it largely immune from competitive pressures that might limit its ability to impose trusted system technology on the market.

[181] Another important policy initiative affecting the enforceability of mass-market licenses of this sort is proposed Article 2B of the Uniform Commercial Code. See generally Symposium: Intellectual Property and Contract Law in the Information Age: The Impact of Article 2B of the Uniform Commercial Code on the Future of Transactions in Information and Electronic Commerce, 13 BERKELEY TECH. L.J. 809 (1998).

[182] If the Pentium III chip ID is designed to allow for copyright protection, as Intel claims it is, it might be a technology which effectively controls access to copyrighted works under Section 1201. If so, it would seem that a hardware device which disables the Processor Serial Number could subject to the anti-device provisions. Take, for example, IBM's new hardware disablement feature: "IBM plans to go the extra step and disable the processor ID feature at the BIOS (or hardware) level in our Pentium III client systems," Letter from Chistopher G. Caine on behalf of IBM Corp. to Jerry Berman, Executive Director of the Center for Democracy and Technology, Jan. 24, 1999, available at http://www.cdt.org/privacy/ibmletter.html.

Under a very strict interpretation of Section 1201(b)(1), either act might be viewed as illegal.[183] It is, however, difficult to believe that most judges would find providing either software or information to enable circumvention of this component of a technical protection system to fall within the DMCA anti-device rules. The DMCA, judges might point out, authorizes circumvention in order to protect personal privacy.[184] While this provision doesn't specifically authorize the development or use of circumvention technologies to accomplish this legitimate act, judges might conclude that Congress must have intended for people to be able to develop or use technology to accomplish the privileged privacy act, or that the Intel identifier was not a component of an effective technical measure. To avert an injustice, judges would likely find an ambiguity in a statute or read in appropriate limiting language. This is clearly not the kind of "black box" circumvention device that Congress had in mind when adopting DMCA.[185] To hold otherwise would, in effect, allow Microsoft to employ the anti-circumvention provisions of DMCA to impose trusted system technology on the public.

It is, of course, an irony that so much of Congressional debate on Section 1201 focused on refining the act of circumvention provision given that the anti-device provisions are, as a practical matter, by far the more important rules in this section.[186] Those who have followed the Clinton Administration's digital copyright policy over the last five years should realize that the anti-device provisions were what the Administration and its major copyright industry allies really cared about. The legislation proposed in the Administration's 1995 White Paper did not include any provision about circumvention of technical protection measures as such.[187] It sought only to outlaw technologies whose "primary purpose or effect" was to enable the circumvention of technical protection measures.[188] Was this lack of attention to circumvention an oversight? Or did the Administration believe that it would be difficult to detect individual acts of circumvention, and as long as such acts were done on an isolated, individual basis, the danger to copyright owners would be small? It is difficult to discern why circumvention as such escaped attention until mid-1997 when the WIPO treaty implementation legislation was first introduced in Congress.[189] Far easier to discern has been the Administration's goal of stopping the manufacture and distribution of technologies with circumvention-enabling uses, either by commercial firms or by technically savvy Robin Hoods.[190]

Eventually someone in the Administration must have realized that it was a bit strange to be proposing to make illegal the manufacture and distribution of technologies whose ordinary uses were not themselves illegal. To justify a broad ban on circumvention technologies, a broad ban on the act of circumvention seemed to be needed. This explains why the Administration and its allies were so insistent that Section 1201(a)(1) be structured to broadly ban acts of circumvention. It also explains why the Administration sought to limit the proliferation of exceptions to the anti-circumvention ban, and why such exceptions as were added to the statute were very narrow. The broader the acknowledged range of legitimate circumventions, the narrower should be an appropriately crafted regulation of circumvention technologies. The Administration may have hoped that in all the hoopla about crafting exceptions to Section 1201(a), Congress would not notice that its seeming recognition of the legitimacy of circumventions for noninfringing purposes in Section 1201(c)(1) might be effectively be nullified by Section 1201(b)(1) which arguably broadly bans technologies necessary to accomplish such circumventions.

---

[183] Posting information on the website might be seen as providing a service to the circumventors.
[184] 17 U.S.C. sec. 1201(i). This provision is extremely complicated and would seem to be very narrow. It is not clear it would apply to the Microsoft example.
[185] See supra notes – and accompanying text and infra note --.
[186] See, e.g., Benkler, supra note --, at [81].
[187] See, e.g., White Paper, supra note 14, at 230-36.
[188] Id., Appendix 1, at 6.
[189] See supra note --.
[190] Professor Benkler likens this strategy to banning VCRs in order to stop home taping. Benkler, supra note --, at [81]. Speaking of VCRs, little noticed in DMCA were its provisions requiring consumer electronics companies to build specific anti-copying technologies into future VCRs. See 17 U.S.C. sec. 1201(k).

When testifying before Congress, proponents of the Administration's anti-device rules repeatedly emphasized that the legislation was needed to stop deliberate and systematic piracy by "black box" providers.[191] Yet, the anti-device provisions adopted by Congress are far broader than this, providing a basis to challenge technologies that have circumvention-enabling uses. This creates a potential for "strike suits" by nervous or opportunistic copyright owners who might challenge (or threaten to challenge) the deployment of a new information technology tool whose capabilities may include circumvention of some technical protection system. No doubt some expert can be found to say that deployment of a particular technology in the market would meet one of the three conditions in the anti-device provisions, giving plausibility to the suit. Weak as such testimony might be, it may be enough to extract a settlement sum from the information technology firm.[192]

The potential for strike suits becomes stronger if one realizes that it is not necessary (or arguably even relevant) to litigation under the anti-device provisions of DMCA whether any act of underlying infringement (e.g., illegal copying of a protected work) has ever taken place. The mere potentiality for infringement will suffice to confer rich rewards on a successful plaintiff. Consider, for example, a recent lawsuit brought by the maker of a proprietary game console against the maker of emulation software that permits games initially developed for the proprietary console to be played on iMac computers.[193] Relying on the DMCA anti-device provision, the plaintiff is seeking up to $25,000 per unit sold in damages because the emulation software allegedly bypasses an anti-copying feature in the games.[194] The plaintiff did not allege or need not prove any actual illicit copying by users of the defendant's emulation software.

The anti-device provisions of Section 1201 are not predictable, minimalist, consistent, or simple, as the Framework principles suggest that they should be. Due to inconsistencies in the statute, it is unclear whether Section 1201's anti-device provisions would be interpreted to allow the development and distribution of technologies to enable legitimate uses, whether or not the legitimate uses are explicitly identified in the statute. Boiled down to its essence, this presents the question of whether Congress should be understood to have made an empty promise of fair use and other privileged circumvention. Unless the anti-device provisions of the DMCA are modified, either by narrow judicial interpretation or by legislative amendments, they are likely to have harmful effects on competition and innovation in the high technology sector. This is not good news for the e-conomy.

VI. POLICYMAKERS SHOULD PERIODICALLY REVIEW BOTH THE ACT AND DEVICE PROVISIONS.

The Administration did not recommend or support inclusion of any provision in the WIPO treaty implementation legislation for any post-legislation assessment of the impact of its anti-circumvention

---

[191] See, e.g., Valenti Testimony, supra note --, at – ("But all security measures, no matter how sophisticated, can be circumvented by clever hackers. Therefore, the law must provide clear and effective sanctions against those who would violate the security of the NII. This requires more than mere civil remedies. Criminal sanctions are essential. Too many NII bandits, some operating totally in the underground economy, will scoff at the threat of civil damages, which many regard as simply a cost of doing business. There must be criminal penalties attached to deliberate, systematic acts of circumvention if such acts are to be seriously lessened."); Testimony of Gail Markels, General Counsel, Interactive Software Association, House Jud. Hearing, supra note 16. See also Letter from Mark Belinsky of Macrovision Corp., House Commerce Hearing, supra note --.

[192] Some commentators even perceive the anti-device rules of Section 1201 as threatening the distribution of many widely used editing and related software tools. See, e.g., Peter Wayner, A New Copyright Law Bans Tools That "Circumvent" Copy Protections. Does That Make Cutting and Pasting Illegal?, Salon Magazine, http://www.salonmagazine.com/21st/.

[193] See Complaint, Sony Computer Entertainment, Inc. v. Connectix Corp., Civ. No. 99-0390 (N.D. Cal.).

[194] Id. at 7-8. This lawsuit is particularly disturbing because the software at issue received a "Best of Show" award at Macworld shortly before the lawsuit was filed. See, e.g., Polly Swenger, Sony Sues Over PlayStation Clone, WIRED NEWS, Jan. 29, 1999, http://www.wired.com/news/print_version/17619.html (visited Jan. 29, 1999).

norms.[195] This might seem surprising in view of the breadth of these norms, their unprecedented character, and their potential impact on both information technology markets and on public access to information. Even if the Administration had initially been unaware of these potential negative impacts, it could not have failed to become aware of them during the legislative process.[196] The Administration was surely aware that the case for the act of circumvention and anti-device norms was long on rhetoric and short on actual evidence of harm to copyright owners.[197] Yet, the Administration did nothing to support post-legislative review of these norms.

This is in striking contrast to the periodic review process endorsed by the Administration as to another legislative initiative affecting e-conomy markets, namely, the proposal to create a new form of legal protection for the contents of databases.[198] Writing on behalf of the Administration concerning its reservations about a bill under consideration in the second session of the 105th Congress, Andrew Pincus, General Counsel to the Commerce Department, stated: "The Administration believes that, given our limited understanding of the future digital environment and the evolving markets for information, it would be desirable for the [database] bill to include a provision for an interagency review of the law's impact at periodic intervals following implementation of the law. This would be consistent with the laws and proposed laws in other emerging technologies where Congress has mandated examination of a new law's economic impact."[199] At least one of the database bills seemingly under consideration in the 106th Congress contains a study provision to assess the impact of the new law.[200] This conforms to the Administration's proposal and to Framework principles. Much the same comment might have been made about the anti-circumvention norms of the DMCA.

Even though the Administration did not support inclusion of study provisions in the DMCA, Section 1201 actually does contain a study provision that will provide an opportunity to review some impacts of the anti-circumvention regulations.[201] In response to the strong concerns expressed by librarians and educators about the potential negative impacts that broad anti-circumvention provisions might have on fair uses of copyrighted works and on access to information and to public domain works,[202] the House Commerce Committee decided that there should be a two-year moratorium on enforcement of the act of anti-circumvention provision.[203] It also proposed a study to determine whether noninfringing uses were being adversely affected by technical protection systems. If so, the Commerce Committee's version of the bill would have waived application of the anti-circumvention norm as to the affected works or users.[204]

---

[195] See, e.g., H.R. 2281, as originally introduced into Congress on July 29, 1997, supra note --; Lehman Testimony, supra note – (endorsing legislation but not asking for a study provision).
[196] See, e.g., Oakley Testimony, supra note --; Greenwood Testimony, supra note --.
[197] See, e.g., sources cited supra notes --. One of the few concrete examples of a device claimed to have contributed to international piracy was that offered in Markels Testimony, supra note – (discussing "Game Doctor" said to have been used to pirate game software).
[198] Letter from Andrew Pincus, General Counsel of the U.S. Dept. of Commerce to Senator Patrick Leahy, Aug. 4, 1998, at 3 (hereinafter "Pincus Letter"). After the House passed the Collections of Information Antipiracy Act, H.R. 2652, Mr. Pincus wrote to Senator Leahy to express the Administration's reservations about the wisdom of this bill and about its constitutionality. Id. at 1.
[199] See Pincus Letter, supra note --, at 3. The letter proposed that "such a study might be conducted under the auspices of the Secretary of Commerce in consultation with the Office of Science and Technology Policy and the Register of Copyrights." Id.
[200] See Congressional Record, 106th Cong., 1st Sess., S316-26, Jan. 19, 1999 (remarks by Senator Hatch, along with the texts of three database bills). See id. at 322 (study provision).
[201] 17 U.S.C. sec. 1201(a)(1)(B)-(D).
[202] See supra note – and accompanying text.
[203] "Commerce Panel Clears Digital Copyright Bill With Further Concessions On Fair Use," 56 BNA Pat., Trademark, & Cop. J. 326, 326 (7/23/98).
[204] Id. As Yochai Benkler has pointed out, this would not stop copyright owners from employing technical protection systems to inhibit noninfringing uses, it would only allow circumvention to obtain access. Benkler, supra note --, at [97].

The Commerce Committee's insistence on the importance of both moratorium and impact study provisions proved surprisingly persuasive. Section 1201(a)(1) (A) provides that the general anti-circumvention ban will not take effect until two years after enactment of the legislation.[205] Subsections (C) and (D) call upon the Librarian of Congress to conduct periodic studies to determine whether certain classes of users or works should be exempt from the ban because technical protection systems are impeding the ability to make noninfringing uses of copyrighted works.[206] Subsection (B) goes on to provide the statutory basis for such an exemption for the classes of works or users determined by the Librarian to be adversely affected by the anti-circumvention norm.[207] The DMCA calls for the first such study to be completed just before the anti-circumvention ban is lifted.[208]

The DMCA directs the Librarian of Congress to consider four factors: "(i) the availability for use of copyrighted works, (ii) the availability for use of works for nonprofit archival, preservation, and educational purposes, (iii) the impact [of] the prohibition…on criticism, comment, news reporting, teaching, scholarship, or research, [and] (iv) the effect of circumvention of technical measures on the market for or value of copyrighted works."[209] The Librarian has authority to consider "such other factors as the Librarian considers appropriate."[210] The DMCA is quite clear, however, that the Librarian's determinations cannot be asserted as a defense to an anti-device claim.[211] Although users would be entitled, after the Librarian's determination, to "hack" technical protection systems for any classes of works whose noninfringing uses had been inhibited, the no-defense-to-an-anti-device-claim subsection would appear to make such user self-help available only if one didn't need to make or use a device to accomplish the act, once again raising the spectre of Congress having created a meaningless privilege. As Professor Benkler has pointed out, the Librarian has no power to tell copyright owners to stop using technical protection systems that are impeding noninfringing uses.[212] Thus, it is quite possible that noninfringing uses will continue to be substantially impeded, notwithstanding the Librarian's determination and rulemaking concomitant to it. Surely, this should be the subject of further study.

While the study provisions in DMCA are surely better than nothing,[213] they fall far short of the periodic review and reporting process appropriate to the unprecedented nature of the circumvention and the anti-device bans.[214] To limit an assessment of the circumvention ban to a certain range of possible effects

---

[205] 17 U.S.C. sec. 1201(a)(1).

[206] The first study is to be completed two years after the date of DMCA's enactment. See 17 U.S.C. sec. 1201(a)(a)(A). Follow-on studies are to be conducted every three years thereafter. See id. at 1201(a)(1)(C). Given how weak was the showing that gave rise to the DMCA's anti-device provisions, it would seem that the showing of interference with lawful uses ought not to be too rigorous. However, the House Manager's report on the legislation would seem to anticipate a relatively high standard of proof. See House Manager's Report, supra note --, at 6-7.

[207] Id. at 1201(a)(1)(B). It appears that any moratorium resulting from such a determination will last for three years. Id. at 1201(a)(1)(D).

[208] Id. at sec. 1201(a)(1)(A). One important question

[209] Id. at 1201(a)(1)(C).

[210] Id.

[211] Id. at 1201(a)(1)(E).

[212] Benkler, supra note --, at [97].

[213] The principal value of the study provisions may well lie in deterring some publishers from egregious uses of technical protection systems that would interfere with fair uses. Another subsection of the DMCA requires the Register of Copyrights and the Assistant Secretary for Communications and Information of the Commerce Department to study the impact of the encryption research exception. See id. at 1201(g)(5).

[214] Among the factors likely to limit the effectiveness of the study system devised in the DMCA is the fact that the Librarian of Congress is apparently supposed to initiate studies of the impact of anticircumvention rules "upon the recommendation of the Register of Copyrights." The Register, in turn, is supposed to consult with an official from the Department of Commerce before recommending a study. 17 U.S.C. sec. 1201(a)(1)(C). It has been a long time since the Registrar of Copyrights or the Commerce Department have taken more than tepid steps to represent the interests of users of copyrighted works, particularly those from the educational and library sectors. Moreover, since none of the Librarian's findings last for more

would ignore the wider swath of harm the act provision may do.[215] Besides, the anti-device ban is the true heart of the anti-circumvention provisions of the DMCA. It is integrally interrelated with the circumvention activity ban.[216] To assess the circumvention ban without considering the anti-device ban is to ignore the most significant technology-regulating provision in the DMCA. Unless construed narrowly, the anti-device provisions may do as much harm to competition and innovation in the information technology industry as the circumvention ban may do to noninfringing academic uses. One would have thought that Congress and the Administration would be concerned about these impacts given that these are the very industries whose tremendous growth the Commerce Department has been trumpeting to the world.[217] The Librarian of Congress should, therefore, decide that his studies can consider the impact of anti-device rules on the ability of certain classes of users or works to make noninfringing uses of protected works.[218] The Librarian should also be entitled to make other observations about possible unintended side-effects of the anti-circumvention regulations that may be detrimental to the public interest.[219]

It is especially important to have periodic reviews of the whole of the anti-circumvention provisions because they sweep so broadly that they may come to be used widely to deal with circumventions far beyond the copyright industry concerns that Congress contemplated. The low level of proof needed to prove anti-circumvention violations,[220] along with the generous remedies the Act provides,[221] may prove to be a magnet for firms to seeking to challenge acts of circumvention or devices that might, for example, concern trade secrecy or computer hacking matters.[222] As long as there is a plausible claim that some material being protected by the technical protection system has a modicum of creative content that would entitle it to copyright protection,[223] any act of circumvention or tool to aid the circumvention might be challenged under Section 1201. Such uses of the statute could make copyright law into a general purpose misappropriation law regulating computer security matters. Moreover, as Section V has shown, Section 1201 is so ambiguous and broad, it may wreak considerable mischief in the information technology field, potentially harming competition and innovation in this important sector. For these reasons, a broad periodic review of the anti-circumvention rules should be undertaken.

VII. CONCLUSION

The WIPO Copyright Treaty provides a "predictable, minimalist, consistent and simple legal environment" that should promote global commerce in electronic information products and services, in line with objectives and principles announced in the Clinton Administration's "Framework for Global Electronic Commerce."[224] As the principal leader in the treaty-making effort that led to conclusion of this treaty, the Clinton Administration deserves credit for promoting this policy initiative that holds promise to substantially benefit the U.S. digital economy industries.

---

than a three year period, copyright industry lobbyists will have multiple opportunities to carve back or eliminate any user-friendly exceptions that the Librarian might have the temerity to recommend.

[215] See supra note – and accompanying text for examples of legitimate circumvention activities unlikely to be captured by the scope of the intended studies by the Librarian.

[216] See supra notes – and accompanying text. See also Benkler, supra note --, at [81].

[217] See supra notes – and accompanying text.

[218] Id. at (a)(1)(C) (setting forth factors). See Benkler, supra note --, at [87] (arguing that "enforcement of the anti-device provision is unconstitutional unless and until the Librarian makes a determination that no noninfringing uses will be adversely affected" by the use of technical protection systems).

[219] See supra notes – and accompanying text for examples of other potential deleterious effects.

[220] See supra notes – and accompanying text.

[221] See 17 U.S.C. sec. 1203(b) (civil remedy provision).

[222] The potential for this was recognized in the Congressional debate over the anti-circumvention rules. See, e.g., Remarks of Rep. Goodblatte, CONG. REC., H7096, Aug. 4, 1998. Although this Congressman indicated that computer hacking statutes should be used to deal with computer hacking problems, there is no reason why someone injured by a computer hacker could not seek relief under Section 1201.

[223] See 17 U.S.C. sec. 102 (copyright protection subsists in all original works of authorship that have been fixed in a tangible medium of expression).

[224] See Framework, supra note 1, at 3.

In most respects, the legislation implementing the WIPO Copyright Treaty in U.S. law conforms to Framework principles as well.[225] The anti-circumvention provisions of the DMCA, however, do not. They are unpredictable, overbroad, inconsistent, and complex. More troubling than the fact that these regulations do not conform to Framework principles is the fact that the many flaws in this legislation will be harmful to innovation and competition in the digital economy sector, as well as harmful to broader public interests. If these regulations are not as maximalist as they were when initially proposed to Congress, this is mainly due to Congress' heeding of concerns expressed by some of the leading firms of digital economy interests, rather than to the Administration's leadership.

In the U.S. Congress, as well as in Geneva during the diplomatic conference leading up to adoption of the WIPO Copyright Treaty, proposed anti-circumvention regulations were contentious. Among the concerns expressed in both venues were these: the potential effect of such rules on public access to information and on the ability to make noninfringing uses of copyrighted works, and their potential effect on competition and innovation in the market for hardware and software products whose uses might include the bypassing of some technical protection systems.[226] The diplomatic conference had the good sense to adopt only a general norm on circumvention activities, leaving nations free to implement this norm in their own way.[227] Thus, the flaws in the DMCA's anti-circumvention provisions do not derive from the treaty, but rather from the bad judgment of the Administration and the major copyright industry groups that urged adoption of these overbroad rules.

This article has demonstrated that the DMCA's ban on the act of circumvention of access controls should have included a general purpose "or other legitimate reasons" provision because the seven exceptions built into the statute, while they respond to the main concerns identified in the legislative debate, do not exhaust the legitimate reasons to bypass access controls.[228] The article has provided examples of other legitimate circumvention activities and has suggested that if Congress does not narrow the reach of this provision, courts likely will do so, even if it involves some stretching to do so.

The article has also demonstrated that the anti-device provisions of the DMCA are substantially overbroad and need to be revised. The intent of Congress was to ban the development and deployment of "black boxes" that promote and enable piracy of copyrighted works.[229] However, the ban is far broader than this and threatens to bring about a flood of litigation challenging a broad range of technologies, even where there is no proof that the technologies have or realistically would be widely used to enable piracy.[230] The legislation is also unclear about a crucial question: whether it is lawful for people to develop or distribute technologies that will enable implementation of the exceptions and limitations on the circumvention ban built into the statute.[231] Did Congress intend to allow people to exercise these privileges, or did it intend to render these privileges meaningless because the technologies to enable the excepted activities have been made illegal? No clear answer to this question emerges from a careful study of the anti-circumvention provisions. While legislative clarification of this issue would be desirable, most likely the courts will have no choice but to address this question. Because of ambiguities in the statute, it is unclear how courts will resolve disputes in which such questions will be posed.

Finally, this article urges that the anti-circumvention provisions be subject to periodic interagency review that would consider its impact as a whole.[232] The DMCA includes a provision authorizing the Librarian of Congress to study the impact of the act of circumvention provision and make a determination about whether this provision is interfering with the ability of certain classes of users to make noninfringing uses of certain classes of copyrighted works.[233] This provision is too narrow in at least two respects. One

[225] See supra notes – and accompanying text.
[226] See supra notes – and accompanying text.
[227] See supra notes – and accompanying text.
[228] See supra notes – and accompanying text.
[229] See supra notes – and accompanying text.
[230] See supra notes – and accompanying text.
[231] See supra notes – and accompanying text.
[232] See supra notes – and accompanying text.
[233] 17 U.S.C. sec. 1201(a)(1)(B).

is that it does not perceive the potential impact of the anti-device bans on the ability of users to make noninfringing uses of copyrighted works. This article has argued that the Librarian of Congress can and should consider this as well.[234] A second is that the DMCA's study provision does not recognize other kinds of potential mischief that the anti-circumvention provisions may do to competition and innovation in the information technology sector.[235] Because of the unprecedented character of the anti-circumvention provisions and their overbreadth, it would be highly desirable for a broader study to be undertaken of the impact of these regulations with an eye to recommending changes to remedy unintended harmful consequences they may be having.

Before concluding this article, it is perhaps worth noting that as yet relatively few classes of copyrighted works are being distributed with technical protection systems built in.[236] Much research and development work is, however, underway to develop such systems.[237] Many copyright owners seem to hope or expect that such systems will be widely used for a broad range of work in the not-too-distant future and that these systems will stop piracy and other unauthorized and arguably unlawful uses of copyrighted works.[238]

One factor that will significantly affect how widely technical protection systems will be deployed and how tight their restrictions on uses of copyrighted works is how consumers will react to them.[239] Copyright owners may feel far more secure if their works are technically protected so well that no unauthorized uses can ever be made of them. However, economists Carl Shapiro and Hal Varian argue that copyright owners must consider this:

> The more liberal you make the terms under which customers can have access to your product, the more valuable it is to them. A product that can be shared with friends, loaned out and rented, repeatedly accessed, or sold in a resale market is obviously more valuable to a potential user than one that can be accessed only once, under controlled conditions, by only a single party.[240]

Moreover, people are very used to being able to make a wide range of uses of copyrighted works without seeking the copyright owner's permission. It is unclear how well they will react to a radical shift in the market for information products. Professor Benkler observes that "[w]e have no idea how a world in which information goods are perfectly excludable—as technical protection measures promise to make them—will look. Because of the non-rival nature of information, prevailing economic theory would suggest that we are as likely to lose as to gain productivity from this technological change."[241] In addition, if consumers won't buy tightly restricted copies, copyright owners may end up worse off than before, rather than better off.[242]

---

[234] See supra notes – and accompanying text.
[235] See supra notes – and accompanying text.
[236] See, e.g., CSTB Intellectual Property Study (forthcoming 1999).
[237] See, e.g., Eric Schlachter, 12 BERKELEY TECH. L.J. 1, 38-45 (discussing various kinds of systems).
[238] See, e.g., Charles Clark, The Publisher in the Digital World, in INTELLECTUAL PROPERTY RIGHTS AND NEW TECHNOLOGIES: PROCEEDINGS OF KNOWRIGHT '95 CONFERENCE 85 (Klaus Braunstein & Peter Paul Sint, ed. 1995). See also White Paper, supra note 14, at 177-90 (foreseeing wide deployment).
[239] Carl Shapiro and Hal Varian assert that "[t]rusted systems, cryptographic envelopes, and other copy protection schemes have their place but are unlikely to pay a significant role in mass-market information goods because of standardization problems and competitive pressures." CARL SHAPIRO & HAL VARIAN, INFORMATION RULES 102 (1998)
[240] Shapiro & Varian, supra note --, at 98.
[241] Benkler, supra note --, at [92].
[242] See, e.g., Branko Geravac, et al., Electronic Commerce and Intellectual Property—Protect Revenues, Not Bits, Address, Forum on Technology-Based Intellectual Property Management: Electronic Commerce for Content (March 7, 1996) (sponsored by the U.S. Copyright Office and the Interactive Multimedia Ass'n).

Competition among information providers may also affect the successful deployment of technical protection systems. If information provider #1 tightly locks up his content, competitive provider #2 may see a business opportunity in supplying a less tightly restricted copy to customers that might otherwise buy from provider #1.[243] A competitive alternative to tight technical controls on content may well be to adopt one or more of the several strategies that Shapiro and Varian discuss as to how content providers can take advantage of the opportunities presented by digital technologies, rather than being overwhelmed by the risks.[244] There are, they say, also many good business models out there waiting to be invented by creative content providers.[245]

If content providers come to believe that a good business model is the best way to protect intellectual property from market-destructive appropriations, perhaps the current debate over the DMCA's anti-circumvention regulations will seem in time like a tempest in a teapot. However, in the meantime, the impact of this legislation should be closely watched because of its potential for substantial unintended detrimental consequences.

[243] This, in essence, what happened when software developers, such as Lotus Development Corp. started distributing copy-protected versions of their programs. Firms with similar products who were willing to sell their products without copy-protection systems attracted enough customers that the leading firms eventually abandoned their technical protection schemes. This is, of course, more likely to occur where markets are competitive and where participants in the market are not acting jointly in deciding on technologies so that consumers will not have a competitive choice.

[244] Id., Chap. 4.

[245] Id. at 84. Some of these business models may themselves be subject to intellectual property protection. See, e.g., Robert P. Merges [paper for the Berkeley e-commerce conference].