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

By Pamela Samuelson †

ABSTRACT

The Digital Millennium Copyright Act of 1998 ("DMCA") prohibits the circumvention of technological protection measures used by copyright owners to control access to their works. It also bans devices whose primary purpose is to enable circumvention of technical protection systems. The Clinton administration proposed these anti-circumvention rules as implementations of U.S. obligations under the World Intellectual Property Organization Copyright Treaty. However, the DMCA's provisions are significantly broader than the treaty required. They violate the Administration's stated goal of only imposing "predictable, minimalist, consistent, and simple" regulations on the budding digital economy.

Although Congress heeded some concerns of digital economy firms by crafting certain exceptions to authorize legitimate circumvention, those exceptions are overly narrow and shortsighted. They should be supplemented by a more general "other legitimate purposes" exception. The DMCA's anti-device provisions are, moreover, overbroad and unclear, especially on the question whether it is legal to develop a technology necessary to engage in a privileged act of circumvention (e.g., a fair use). Either Congress or the courts will be forced to constrain the reach of the anti-device rules so as not to undermine Congressional intent to preserve fair uses and so as not to harm competition and innovation in the information technology sector. Finally, though the DMCA provides

---

† 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 that 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 derivative work of that paper. Although that project was never completed, this article builds on the base of that collaboration. I am also grateful for comments on this draft from Hal Abelson, Jonathan Band, Yochai Benkler, Julie Cohen, Gideon Frieder, Joan Feigenbaum, Bob Glushko, Peter Huang, Laurel Jamtgaard, and Kurt Opsahl.

for a study of one class of potentially harmful impacts of the anti-circumvention rules, this study needs to be broadened to consider the full impact of this unprecedented legislation.

TABLE OF CONTENTS

I. 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 digital economy, and argues for international cooperation in adopting consistent policies that will promote this commerce.[2] The Commerce Department's *First Annual Report* on the Framework initiative indicates that this initiative has

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. *See id.* at 2-4.

met with some success.[3] Passage of the Digital Millennium Copyright Act ("DMCA")[4] 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 World Intellectual Property Organization ("WIPO") Copyright Treaty[6] in the international community.[7] This treaty establishes several important international norms for applying copyright law in the digital environment.[8] International consensus on these norms should aid the growth of the global digital economy.[9] However, the DMCA was largely unnecessary to implement the WIPO Copyright Treaty because U.S. law already complied with all but one minor provision of that treaty.[10]

Although the WIPO Copyright Treaty requires countries to provide "adequate protection" against the circumvention of technical measures used by copyright owners to protect their works from infringement, the DMCA went far beyond treaty requirements in broadly outlawing acts of circumvention of access controls and technologies that have circumvention-enabling uses.[11]

---

3. *See* U.S. GOV'T WORKING GROUP ON ELEC. COMMERCE, FIRST ANNUAL REPORT (1998), *available at* <http://www.doc.gov/ecommerce/E-comm.pdf> [hereinafter FIRST ANNUAL REPORT].

4. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998).

5. *See* FIRST ANNUAL REPORT, *supra* note 3, at 2.

6. *See* WIPO Copyright Treaty, adopted by the Diplomatic Conference on Dec. 20, 1996, WIPO Doc. CRNR/DC/94 (Dec. 23, 1996) [hereinafter 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 on Dec. 20, 1996, WIPO Doc. CRNR/DC/95 (Dec. 23, 1996). 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.

7. *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).

8. See *infra* notes 45-55 and accompanying text for a discussion of these norms.

9. *See* FIRST ANNUAL REPORT, *supra* note 3, at 10-11.

10. *See, e.g.*, Pamela Samuelson, *Big Media Beaten Back*, WIRED, March 1997, at 64 (explaining that U.S. law was in compliance with almost all norms of the treaty). Only the treaty provision calling for protecting the integrity of rights management information needed legislative implementation in U.S. law. WIPO Copyright Treaty, *supra* note 7, art. 12; *see also infra* notes 56-64 and accompanying text.

11. WIPO Copyright Treaty, *supra* note 6, art. 11. The DMCA anti-circumvention provision can be found at 17 U.S.C.A. § 1201 (West Supp. 1999). See *infra* notes 66-70

The anti-circumvention rules in the DMCA do not match up well with the needs of the digital economy, or with the principles propounded in the Framework.[12] Although the *First Annual Report* praises the DMCA for the balance it embodies between copyright protection and access to information,[13] this article will demonstrate that such balance as the DMCA contains is attributable to congressional foresight, not to the Clinton Administration.[14] Indeed, for the past five years, the Administration has supported highly unbalanced digital copyright initiatives and has resisted most efforts to introduce more balance in these initiatives.[15] With the enactment of the anti-circumvention provisions of the DMCA, the Administration may have had more success in achieving imbalance in digital copyright law than Congress may have realized.[16]

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.[17] Hollywood and its allies sought the strongest possible ban both on the act of circum-

---

and accompanying text for a discussion of why the treaty did not require the DMCA provisions.

12. See *infra* Part III for an articulation of these principles. See *infra* Parts V-VIII for an analysis of why these provisions may be harmful to digital economy interests.

13. *See* FIRST ANNUAL REPORT, *supra* note 3, at 14.

14. *See infra* Part V.

15. *See* U.S. DEP'T OF COMMERCE INFO. INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS (1995) [hereinafter *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 OR. 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 Protection and Emerging Computer Technology*, 41 VILL. L. REV. 207 (1996); Pamela Samuelson, *The Copyright Grab*, WIRED, Jan. 1996, at 134.

16. *See infra* Parts V-VII.

17. *See, e.g.*, *WIPO Copyright Treaties Implementation Act; and Online Copyright Liability Limitation Act: Hearing on H.R. 2281 and H.R. 2280 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary* 105th Cong. 78-82 (1997) [hereinafter *Judiciary Hearing*] (statement of Jack Valenti, President and CEO, Motion Picture Ass'n of America); *id.* at 256-65 (statement of Edward J. Black, President, Computer and Communications Industry Ass'n). 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 later in this article. *See infra* notes 180-186 and accompanying text. *See also Judiciary Hearing*, *supra*, at 68-77 (statement of Robert W. Holleyman II, President, Business Software Alliance).

venting a technical protection system used by copyright owners to protect their works and on technologies having circumvention-enabling uses.[18] 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.[19] They supported legislation to outlaw acts of circumvention engaged in for the purpose of infringing copyrights and would have supported narrowly drawn device legislation had the Congressional subcommittees principally responsible for formulating WIPO treaty implementation legislation been receptive to a narrower bill.[20] Silicon Valley and its allies warned of dire consequences if the overbroad anti-circumvention provisions Hollywood supported were adopted.[21] 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.[22]

Had the Administration sought to broker a fairer compromise between the interests of Hollywood and its allies and the interests of 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 infor-

---

18. *See, e.g., Judiciary Hearing, supra* note 17, at 78-82 (statement of Jack Valenti); *id.* at 204-12 (statement of Allan R. Adler, Vice President for legal and governmental affairs, Ass'n of American Publishers).

19. *See infra* notes 87-94 and accompanying text. Other groups opposed to the broad anti-circumvention legislation of H.R. 2281 included librarians and educators. *See infra* notes 117-120 and accompanying text.

20. The Digital Future Coalition—whose members include the Computer & Communications Industry Association, among other high tech industry groups—endorsed H.R. 3048, 105th Cong. (1997), which proposed such a narrow circumvention provision. *See Introduction of the Digital Era Copyright Enhancement Act*, 55 BNA PAT., TRADEMARK & COPYRIGHT J. 68, 70-71 (1997) (describing the anti-circumvention provision of H.R. 3048). *See also Judiciary Hearing, supra* note 17, at 256-65 (statement of Edward J. Black) (critical of the Administration's anti-circumvention proposal); *id.* at 249-56 (statement of Chris Byrne, Director of Intellectual Property, Silicon Graphics, Inc., on behalf of the Info. Tech. Indus. Council) (critical of H.R. 2281).

21. *See, e.g., Judiciary Hearing, supra* note 17, at 260 (prepared statement of Edward J. Black); *see also id.* at 154-55 (prepared statement of Prof. Robert L. Oakley, Georgetown University Law Center).

22. *See infra* Part V.

mation technology sector, that the Administration would have taken a more balanced position on these issues.[23] 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.[24]

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's act-of-circumvention provision expressly recognizes.[25] This provision 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 act-of-circumvention prohibition.[26] 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, periodic reviews of the impact of the anti-circumvention provisions of the DMCA as a whole should be undertaken.[27] Given how broad the anti-circumvention rules are, given their unprecedented character, and given the potential for harmful consequences from these rules, 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.

---

23. *See infra* Part III.

24. *See* 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*, 74 N.Y.U. L. REV. 354 (1999).

25. *See infra* Part VI.

26. *See infra* Part VII.

27. *See infra* Part VIII.

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

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

> During the past few years, the United States economy has performed beyond most expectations. A shrinking budget deficit, low interest rates, a stable macroeconomic environment, expanding international trade with fewer 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 creating this 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 computing power and communication and information technology appear to have been a major force behind this beneficial trend."[28]

This report indicates that the IT sector of the U.S. economy—which includes the computer hardware, software, networking and telecommunications industries—now constitutes an estimated 8.2 per cent of the gross domestic product, close to twice its share of GDP as compared with a decade or so before.[29] The IT sector, moreover, accounts for more than one-quarter of the real economic growth in the American economy.[30] Approximately 45 per cent of current expenditures on business equipment are investments in IT products and services.[31] 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, nearly a fifty-fold increase in only a dec-

28. U.S. DEP'T OF COMMERCE, SECRETARIAT ON ELEC. COMMERCE, THE EMERGING DIGITAL ECONOMY 1 (1998) [hereinafter EMERGING DIGITAL ECONOMY].

29. *See id.* at 4.

30. *See id.* at 6.

31. *See id.*

ade.[32] Perhaps somewhat more wondrous are the astonishing market capitalizations of relatively new Internet firms, such as Amazon.com, Yahoo!, and E*Trade. 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.[33] It is, of course, important to realize that the IT sector is not the only component of the digital economy.[34] 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.[35] Especially as electronic commerce via the Internet and the World Wide Web expands, the IT sector is likely to experience further explosive growth.[36]

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 the growth potential of the digital economy.[37] 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."[38] One of the signal achievements of the Framework was the promulgation of five principles that 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.

---

32. *See 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.

33. *See, e.g.*, James J. Cramer, *TulipMania.com? Despite their soaring prices, the best Internet stocks are still bargains. Here's how to pick 'em*, TIME, Aug. 3, 1998, at 77; *see generally* Steve Mott, *Where Eagles Soar: Making Sense of Internet Valuations*, BUSINESS 2.0, Nov. 1998.

34. *See* EMERGING DIGITAL ECONOMY, *supra* note 28, chs. 4-5 (discussing digital economy sectors).

35. *See id.*

36. *See id.*

37. *See id.* at 50-51.

38. FRAMEWORK, *supra* note 1, at 2; EMERGING DIGITAL ECONOMY, *supra* note 28, 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.[39]

The *First Annual Report* of the U.S. Working Group on Electronic Commerce offers evidence that the Framework's policy objectives are being achieved.[40]

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.[41] However, it has been widely criticized by the IT/digital economy sector for not following these principles in the security/encryption policy area and in the content policy area, owing to the Administration's support for the Clipper Chip and the Communications Decency Act.[42] 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 reconstruct the legal infrastructure of the digital environment so that it would accommodate their preferences. These industries insisted that this restructuring was necessary to protect them from the grave threat of piracy posed in the digital environment.[43] Many significant players in the existing digital economy counseled against this restructuring.[44] 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 partici-

---

39. FRAMEWORK, *supra* note 1, at 2-3.

40. *See id.* at iii-v.

41. *See id.* at iii, 7 (mentioning passage of the Internet Tax Freedom Act); *see also id.* at 12 (discussing foreign tax initiatives).

42. *See, e.g.*, ESTHER DYSON, RELEASE 2.0 (1997).

43. *See Judiciary Hearing*, *supra* note 17, at 79-80 (prepared statement of Jack Valenti).

44. *See id.* (testimony of Edward J. Black; testimony of Chris Byrne); *see also The WIPO Copyright Treaties Implementation Act: Hearing on H.R. 2281 Before the Subcomm. on Telecomm., Trade, & Consumer Protection of the House Comm. on Commerce*, 105th Cong. (1998) [hereinafter *Commerce Hearing*].

pating 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.

III. 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.[45] They include:

1) copyright owners should have an exclusive right to control the making of copies of their works in digital form,[46]

2) copyright owners should have an exclusive right to control the communication of their works to the public,[47]

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,[48]

---

45. *See* WIPO Copyright Treaty, *supra* note 7. *See also* Samuelson, *supra* note 7 (discussing the digital agenda WIPO treaty provisions).

46. There was an explicit provision on the reproduction right in the draft treaty initially considered at WIPO. *See* Basic Proposal For the Substantive Provisions of the Treaty On Certain Questions Concerning the Protection of Literary and Artistic Works To Be Considered at the Diplomatic Conference, WIPO Doc. CRNR/DC/4, art. 7(1) (Aug. 30, 1996). However, this provision did not attract consensus because of its inclusion of temporary reproductions, which was highly controversial. *See* Samuelson, *supra* note 7, at 382-90. 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 Dec. 20, 1996, WIPO Doc. CRNR/DC/96 at 1 (Dec. 23, 1996) [hereinafter Agreed Statements]. For a discussion of the tortured history of the draft treaty provision, the Agreed Statements, and what they mean, see Samuelson, *supra* note 7, at 382-92.

47. *See* WIPO Copyright Treaty, *supra* note 6, art. 8. While the United States does not have an exclusive right of communication in its copyright law, *see* 17 U.S.C. § 106 (1994) (exclusive rights provisions), its public performance and distribution rights are substantively equivalent to this right. *See id.;* Samuelson, *supra* note 7, at 392-98 (discussing negotiations concerning digital communications).

48. *See* Agreed Statements, *supra* note 46, 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* Samuelson, *supra* note 7, at 398-409 (discussing the draft and final provisions on fair use and other exceptions). Although the White Paper had expressed doubts about the vi-

4) merely providing facilities for the communication of works should not be a basis for infringement liability,[49]

5) it should be illegal to tamper with copyright management information insofar as this would facilitate or conceal infringement in the digital environment,[50] 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 infringing uses.[51]

To the extent that uncertainties about how copyright law should apply in the digital environment were impeding the growth of a global market in electronic intellectual property products,[52] there was reason to be optimis-

---

ability 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 15, at 82; Samuelson, *supra* note 7, at 406.

49. *See* Agreed Statements, *supra* note 46, 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 15, at 114-24; Samuelson, *supra* note 7, 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.A. § 512 (West Supp. 1999).

50. *See* WIPO Copyright Treaty, *supra* note 7, art. 12. For a discussion of the history and meaning of this provision, see Samuelson, *supra* note 7, at 415-18.

51. *See* WIPO Copyright Treaty, *supra* note 7, art. 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. *See* Samuelson, *supra* note 7, at 409-15.

52. 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), *available at* <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 COMM'N ON NEW TECHNOLOGICAL USES OF COPYRIGHTED WORKS, FINAL

tic that conclusion of this treaty would remove these blockages and allow e-commerce to flourish.[53] These norms are as "predictable, minimalist, consistent, and simple" components of a legal environment for commerce as one could expect copyright professionals to devise.[54] Thus, the WIPO treaty itself established 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.[55] 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.[56] Its cases had already recognized the rights of authors to control digital reproductions of their works,[57] as well as to control digital transmissions of their works to the public.[58] Courts had invoked fair use in a number of digital copyright cases,[59] and had refused to hold online service providers liable for infringing activities of users about which the providers had no knowledge.[60] Because of the substantial accord between the WIPO treaty norms and existing U.S. law, the Clinton Administration initially considered whether the WIPO Copyright Treaty might even be sent to the Senate for ratification "clean" of implementing legislation.[61] This would have avoided the kind of protracted legislative battle that oc-

---

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* Samuelson, *supra* note 7, at 382-85 (discussing lack of clarity about the reproduction right in the digital environment).

53. *See, e.g.*, FIRST ANNUAL REPORT, *supra* note 3, at 13-14.

54. FRAMEWORK, *supra* note 1, at 3.

55. *See* List of Participants, WIPO Doc. No. CRNR/DC/INF.2 (Dec. 20, 1996).

56. 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* Samuelson, *supra* note 7, at 434-37.

57. *See, e.g.*, Sega Enterprises, Ltd. v. MAPHIA, 857 F. Supp. 679 (N.D. Cal. 1994).

58. *See, e.g.*, Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993).

59. *See, e.g.*, Lewis Galoob Toys, Inc. v. Nintendo of America, 964 F.2d 965 (9th Cir. 1992) (software enabling temporary changes in the play of Nintendo games held fair use).

60. *See, e.g.*, Religious Tech. Center v. Netcom Online Comm. Corp., 907 F. Supp. 1361 (N.D. Cal. 1995) (online service provider should not be held strictly liable for user infringement of which it had no knowledge).

61. *See Clinton Administration Is Undecided On Implementing Steps For WIPO Treaties*, 53 BNA PAT., TRADEMARK & COPYRIGHT J. 241 (1997).

curred when Congress considered the Administration's White Paper legislation in 1996.[62] 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.[63] The DMCA implementation of this norm, which closely tracks the treaty language, was uncontroversial during the legislative process.[64]

The U.S. could have asserted that its law already complied with the WIPO treaty's anti-circumvention norm.[65] This norm was, after all, very

---

62. *See* Samuelson, *supra* note 7, at 427-32 (arguing that U.S. efforts at WIPO conference were aimed at bypassing contention over domestic legislative proposals).

63. *See* WIPO Copyright Treaty, *supra* note 7, 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* Julie E. Cohen, *Some Reflections on Copyright Management Systems and Laws Designed to Protect Them*, 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...." WIPO Copyright Treaty, *supra* note 6, art. 12. Section 43(a) would not seem to cover misrepresentations of this sort. *See* 15 U.S.C. § 1125(a) (1994); *see also* 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., at 3-4 (1998) [hereinafter House Manager's Report].

64. *See* 17 U.S.C.A. § 1202 (West Supp. 1999). 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 copyright management information ("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.

65. It is far more plausible that the U.S. is in compliance with the WIPO treaty anti-circumvention 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 for the Protection of Literary and Artistic Works, Sept. 9, 1886, art. 6*bis* (Paris Text, 1971, amended 1979), *reprinted in* 1 BASIC DOCUMENTS OF INT'L ECON. L. (CCH) 715 (1994). *See also* Jessica Litman, *The Tales That Article 2B Tells*, 13 BERKELEY TECH. L.J. 931, 932 (1998) (discussing the U.S. rationale for claiming to be in compliance with the Berne Convention's moral rights provision, and expressing skepticism about the adequacy of this rationale). *See also* Jonathan Band & Taro

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.[66] With U.S. copyright industries thriving in the current legal environment, it would have been fair to conclude that copyright owners already were adequately protected by the law.[67] 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.[68] 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.[69] However, the political reality and legislative dynamics of the WIPO Copyright Treaty implementation process were such that some sort of anti-circumvention provision appeared to be a necessary part of the bill.

Even if a reasoned assessment of U.S. law might have 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"

Isshiki, *The New Anti-Circumvention Provision in the Copyright Act: A Flawed First Step*, 3 CYBERSPACE LAW. 2 (1999) (explaining that the DMCA's anti-circumvention regulations were not required for compliance with the WIPO Copyright Treaty).

66. *See* White Paper, *supra* note 15, 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).

67. *See, e.g.*, *Judiciary Hearing*, *supra* note 17, at 78 (statement of Jack Valenti) (citing $60 billion in annual U.S. revenues from international sales of intellectual property and naming copyright industry as single greatest contributor to U.S. economy); Motion Picture Ass'n of America Research Dep't, *MPAA 1998 U.S. Economic Review* (visited Apr. 22, 1999) <http://www.mpaa.org/useconomicreview/1998/index.htm> (demonstrating steadily increasing U.S. box office receipts between 1991 and 1998).

68. *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).

69. *See* Ejan Mackaay, *The Economics of Emergent Property Rights on the Internet*, *in* THE FUTURE OF COPYRIGHT IN A DIGITAL ENVIRONMENT 13, 21 (P. Bernt Hugenholtz ed., 1996). "It is this restraint," says MacKaay, "that guards us from sliding into rent-seeking." *Id.* at 22.

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. Silicon Valley Representative Tom Campbell proposed such an approach in his alternative bill.[70] If this same assessment caused policymakers to decide there was also a need for some regulation of circumvention technologies to promote electronic commerce, then 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.[71] Many "digital economy" firms and organizations supported the first of these proposals,[72] and they would likely have supported the second if it had ever had a chance of being taken seriously.

Clinton Administration officials, bowing to the wishes of Hollywood and its allies, 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 this article.[73] It 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 indus-

---

70. *See* H.R. 3048, 105th Cong. § 8 (1997). Northern Virginia Representative Rick Boucher (whose district includes America Online) cosponsored this bill.

71. 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).

72. *See supra* note 20.

73. 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, e.g.*, 17 U.S.C. § 104A (1994) (restoration of 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. §§ 111-112 (1994) (effective Jan. 1, 1978) (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 the new anti-circumvention regulations affect a broad range of industries. This makes the incomprehensibility of the provisions more troublesome.

tries. 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.[74] They also seem to think they are entitled to control the design and manufacture of all information technologies that can process digital information.[75] The DMCA caters to their interests far more than to the interests of the innovative information technology sector or of the public.

IV. 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 focuses on the act of circumvention. Section 1201(a)(1)(A) generally outlaws the act of circumventing "a technological measure that effectively controls access to a work protected under this title."[76] 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.[77] When it does come into force, it will be subject to seven complex exceptions that will be discussed below in Part V.A.[78]

Section 1201 also contains two "anti-device" provisions. Sections 1201(a)(2) and 1201(b)(1) both regulate technologies with circumvention-enabling capabilities. The former focuses on devices that circumvent "a technological measure that effectively controls access to a [copyrighted] work" (access controls).[79] The latter relates to devices that circumvent the "protection afforded by a technological measure that effectively protects a

---

74. *See* Samuelson, *supra* note 15 (discussing the copyright maximalist agenda the Clinton Administration has supported).

75. 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*, WIRED, March 1997, at 61, 186 ("Japan and other Asian 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.A. § 1201(k).

76. 17 U.S.C.A. § 1201(a)(1)(A).

77. *See id.*; *infra* notes 208-210 and accompanying text.

78. *See id.* § 1201(d)-(j), discussed *infra* notes 98-135 and accompanying text.

79. *Id.* § 1201(a)(2); *see also id.* § 1201(a)(3) (defining the phrases "circumvent a technological measure" and "effectively controls access to a work").

right of a copyright owner ... in a work or a portion thereof" (e.g., copy controls).[80] In each case, 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"[81] if it (1) "is primarily designed or produced for the purpose of circumventing,"[82] (2) "has only limited commercially significant purpose or use other than to circumvent,"[83] or (3) "is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing"[84] the technological measure or the protection it affords. The anti-device rules have a narrower range of exceptions than does the act-of-circumvention ban.[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 than the DMCA as enacted. The original proposal would have outlawed circumventions of technical protection systems except when done for legitimate law enforcement or intelligence purposes.[86] However, representatives of major information technology firms and organizations brought to Congress's attention that this norm would interfere with many legitimate activities.[87] It would, for example, have outlawed encryption research and computer security testing, even though these activities are critical to achieving many of the ob-

---

80. *Id.* § 1201 (b)(1); *see also id.* § 1201(b)(2) (defining the terms "circumvent protection afforded by a technological measure" and "effectively protects a right of a copyright owner under this title").

81. *Id.* § 1201(a)(2), (b)(1).

82. *Id.* § 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.* § 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 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) (on file with author).

84. 17 U.S.C.A. § 1201(a)(2)(C), (b)(1)(C).

85. *See id.* § 1201(g)(4), (j)(4).

86. *See* H.R. 2281 § 1201, 105th Cong. (1997) (as introduced in the House of Representatives on July 29, 1997), *reprinted in* 54 BNA PAT., TRADEMARK & COPYRIGHT J. 270 (1997).

87. *See, e.g., Judiciary Hearing, supra* note 17, at 256-61 (statement of Edward J. Black).

jectives of the digital economy.[88] 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 digital economy.[89]

These same firms and organizations, in alliance with major consumer electronics firms, were also critical of the Administration's preferred anti-device provisions.[90] However, these digital economy groups exhausted their political capital on getting critical exceptions to the act-of-circumvention ban[91] and on establishing 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.[92] They took some comfort in statements by Congressional supporters of a limited interpretation of the anti-device norms indicating that Congress meant for the anti-device provisions to apply to "'black boxes' that are expressly intended to facilitate circumvention."[93] Still, the digital economy sector remains understandably concerned about the potential for overbroad application of

88. *See* Letter from Dr. Charles Brownstein, Chair of the Public Policy Committee of the U.S. Chapter of the Association for Computing Machinery, to Rep. Thomas J. Bliley, Chairman of the House Commerce Committee (Sept. 29, 1998) (on file with author) (expressing concern about impact of broad anti-circumvention regulations on computer security research). *See also* FRAMEWORK, *supra* note 1, § 6 (emphasizing the importance of computer security to the growth of global economic commerce).

89. *See infra* Part V.

90. *See Commerce Hearing*, *supra* note 44, at 32-33 (prepared statement of Chris Byrne, Director of Intellectual Property, Silicon Graphics, Inc., on behalf of Info. Tech. Indus. Council); *id.* at 28-30 (statement of Jonathan Callas, Chief Technology Officer, Network Assocs., Inc.); *id.* at 58-63 (statement of Seth Greenstein, Esq., on behalf of the Digital Media Ass'n); *id.* at 46-49 (statement of Walter H. Hinton, Vice President, Storage Tech. Corp., on behalf of the Computer and Communications Indus. Ass'n); *id.* at 18-27 (statement of Gary J. Shapiro, Chairman, Home Recording Rights Coalition, and President, Consumer Elecs. Mfrs. Ass'n).

91. *See* 17 U.S.C.A. § 1201(f), (g), and (j).

92. *See id.* § 1201(c)(3); 144 CONG. REC. H7093, H7095 (daily ed. Aug. 4, 1998) (statement of Rep. Bliley).

93. *See id.* at H7094-95 ("This provision is not aimed at products that are capable of commercially significant noninfringing uses...."). *See also id.* at H7097 ("[I]t is not enough for the primary effect of the device to be circumvention. It, therefore, excludes legitimate multipurpose devices...."); House Manager's Report, *supra* note 63, 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."); *infra* note 192 and accompanying text.

the anti-circumvention and anti-device norms, and recent developments suggest that there is reason for this concern.[94]

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.[95] Proponents of the Administration's preferred anti-circumvention regulations scoffed at arguments made by an alliance of consumer electronics firms and by representatives of the computer and software industries about the harm that broad anti-circumvention regulations would do in this industry.[96] 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.[97]

V. THE ENUMERATED EXCEPTIONS IN THE ACT-OF-CIRCUMVENTION BAN ARE UNDULY NARROW AND INCONSISTENT WITH FRAMEWORK PRINCIPLES

A. The Statutory Exceptions to the Circumvention Ban

The DMCA ban on the act of circumventing technical protection systems is subject to seven very specific exceptions,[98] as well as being qualified by several other subsections.[99] 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.[100] While several of these exceptions and limitations respond to the gravest of concerns expressed by digital economy firms,[101]

---

94. *See infra* notes 193-195and accompanying text.

95. *See, e.g., House Subcommittee Holds Hearings on WIPO Treaty Bills, OSP Liability*, 54 BNA PAT., TRADEMARK & COPYRIGHT J. 414 (1997).

96. *See, e.g., Judiciary Hearing, supra* note 17, at 204-12 (statement of Allan Adler).

97. *See, e.g., id.* at 229, 235-36 (testimony of Michael K. Kirk, executive director, American Intellectual Property Law Ass'n).

98. *See* 17 U.S.C.A. § 1201(d)-(i) (West Supp. 1999).

99. *See id.* § 1201(c)(1)-(4).

100. *See id.* § 1201(a)(1)(A)-(C).

101. *See id.* § 1201(f) (reverse engineering exception), 1201(g) (encryption research), and 1201(j) (computer security testing). *See also Judiciary Hearing, supra* note 17, at 260-61 (prepared statement of Edward J. Black) (expressing concern about reverse engi-

they are still too narrowly crafted, as examples given below will reveal.[102] 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 it 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 provision and its complexity resulted from the maximalist position with which the Administration and its major copyright industry allies began the legislative struggle. Only when IT 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.[103] As noted above, Clinton Administration officials initially sought an almost unlimited ban of circumvention activities.[104] The only exception to the circumvention ban in the Administration's favored legislation was an authorization of 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 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 copy-

---

neering); *Commerce Hearing*, *supra* note 44, at 29-30 (prepared statement of Jonathan Callas) (expressing concern about encryption and security research).

102. *See infra* Part V.B.

103. *See supra* note 101.

104. *See* Band & Isshiki, *supra* note 65 (indicating that Patent and Trademark Office (PTO) officials had initially sought to outlaw circumvention of copy controls, as well as of access controls, and that lobbying by library and educational groups had persuaded Commerce Department officials to drop this provision of the PTO's preferred bill).

105. *See* H.R. 2281 § 1201(e), 105th Cong. (1997) (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.A. § 1201(e) (West Supp. 1999).

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 § 1201(a)(1).

right 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 did not directly say so.[108] 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 should 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 aimed at the former, not the latter. Fair use, for example, would provide a poor

---

107. H.R. 2281 § 1201(d) (as introduced in the House of Representatives on July 29, 1997). *See* 17 U.S.C.A. § 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 Judiciary Hearing*, *supra* note 17, at 235-36 (testimony of Michael K. Kirk).

109. *See also* White Paper, *supra* note 15, 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. *Judiciary Hearing*, *supra* note 17, at 208 (prepared statement of Allan Adler). 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* House Manager's Report, *supra* note 63, at 5 (characterizing circumvention to get unauthorized access as "the electronic equivalent to breaking into a locked room to obtain a copy of a book"). *But see, e.g.*, Friedman, *supra* note 68, 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* Cohen, *supra* note 63, at 174-76 (discussing lawful circumvention); *see also* Julie E. Cohen, *Copyright and The Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089, 1142 n.200 (1998) (finding in copyright's fair use doctrine an affirmative right to "hack" technical protection systems to make fair uses).

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 of that copy, this would appear to be lawful under section 1201(a)(1) and (c)(1).[113] Take, for example, an act of circumvention performed by Geoffery Nunberg, a friend of mine who works for Xerox's Palo Alto Research Center. He was an expert witness in a lawsuit which successfully challenged the Washington Redskins' trademark on the ground that the word "redskins" is scandalous or disparaging.[114] Nunberg 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. 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 circum-

113. *See* 144 CONG. REC. H7097 (daily ed. Aug. 4, 1998) (letter from Rep. Howard Coble to Rep. Rick Boucher) (indicating an intent to distinguish between circumvention to get unauthorized access to a work and circumvention to make fair uses).

114. *See* Harjo v. Pro-Football, Inc., 45 U.S.P.Q.2d (BNA) 1789 (1998); 15 U.S.C. § 1052(a) (1994) (excluding scandalous and disparaging matter from trademark protection); *See also "Redskins" Mark is Cancelled as Disparaging to Native Americans*, BNA PAT., TRADEMARK & COPYRIGHT LAW DAILY (Apr. 12, 1999).

115. *See, e.g.*, 144 CONG. REC. H7093 (daily ed. Aug. 4, 1998) (statement of Rep. Bliley) (indicating that the Commerce Committee understood the legislation to enable consumers to "exercise their historical fair use rights"); *see also id.* at H7097 (letter from Rep. Coble to Rep. Boucher).

116. But see *infra* notes 157-162 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.*, *Commerce Hearing*, *supra* note 44, at 64-66 (statement of Prof. Robert L. Oakley).

vent 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 because vendors of technically protected copyrighted works will 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]

Computer and software industry groups were initially unsuccessful in persuading Congress to create 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.[121] Not until the full Senate Judiciary Committee and the House Commerce Committee undertook their reviews of the legislation were 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

---

118. *See* 17 U.S.C.A. § 1201(d) (West Supp. 1999).

119. *See infra* notes 151-156 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., Judiciary Hearing, supra* note 17, at 148-56 (statement of Robert L. Oakley); *id.* at 64-68 (statement of M.R.C. Greenwood, chancellor of the University of California, Santa Cruz) (expressing concerns about the impact of technical protection systems on noninfringing uses of protected works—concerns the "shopping privilege" does not address).

121. *See, e.g., id.* at 256-65 (statement of Edward J. Black) (expressing concern about the impact of the anti-circumvention provisions for achieving interoperability among computer programs).

122. *See* 17 U.S.C.A. § 1201(f) (West Supp. 1999).

123. *See id.* § 1201(c)(3).

124. *See id.* § 1201(c)(2).

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 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 to circumvent access controls when necessary to protect their children from accessing harmful 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

125. *See Commerce Hearing*, *supra* note 44, at 1-3 (statement of Rep. Tauzin, Subcomm. Chairman) (explaining the Commerce Committee's reasons for reviewing the WIPO treaty implementation legislation).

126. *See Commerce Panel Clears Digital Copyright Bill With Further Concessions on Fair Use*, 56 BNA PAT., TRADEMARK & COPYRIGHT J. 326 (1998).

127. This eventually was codified in the DMCA. *See* 17 U.S.C.A. § 1201(g) (West Supp. 1999).

128. These were also eventually codified in the DMCA. *See id.* § 1201(h), (i).

129. *See id.* § 1201(a)(1)(B). See also *infra* notes 205-206 and accompanying text for discussion of this provision.

130. 144 CONG. REC. H7094 (daily ed. Aug. 4, 1998) (statement of Rep. Bliley).

131. *See* 17 U.S.C.A. § 1201(a)(1)(B)-(D). *See infra* notes 203-210 and accompanying text.

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]

B. Circumvention for Other Legitimate Reasons Should Be Privileged

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 demonstrate that section 1201 should have an "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 protect 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 course of a dispute about the performance quality of this software, the content producer might with-

---

132. 144 CONG. REC. H7094 (daily ed. Aug. 4, 1998) (statement of Rep. Bliley).

133. 17 U.S.C.A. § 1201(c)(4).

134. *Compare* H.R. 2281, 105th Cong. (1998) (as passed on Aug. 4, 1998), *with* Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998).

135. *See* 17 U.S.C.A. § 1201(j). This too had been the subject of testimony before the House Commerce Committee. *See Commerce Hearing*, *supra* note 44, at 27-30 (statement of Jonathan Callas).

hold 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 the software from operating.[136] To deal with this development, the licensee might well attempt to circumvent the self-help feature now 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 licensor breach to justify 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.

Two further 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 other 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, without getting the producer's permission or over the

136. Software developers can embed specialized disabling subprograms in licensed software. These may cause the software to cease 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 Pamela Samuelson, *Embedding Technical Self-Help in Licensed Software*, 40 COMM. ACM 13 (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 interests. *See* U.C.C. § 2B-716 (Feb. 1999 Draft). *See also* Memorandum from Susan H. Nycum to Uniform Commercial Code Article 2B Reporter and Drafting Committee regarding Licensor Self-Help Revision of Proposed UCC 2B, at 1 (Jan. 27, 1997) *available at* <http://www.2bguide.com/docs/nycshelp.html> (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"); Memorandum from Michele Kane on behalf of Walt Disney Co. to Prof. Raymond T. Nimmer, Reporter for Article 2B, at 3 (Jan. 27, 1997), *available at* <http://www.2bguide.com/docs/mkane.html> (strenuously objecting to Article 2B's endorsement of technical self-help provisions in model licensing law as "unnecessary and unfair").

138. *See* 17 U.S.C.A. § 1201(i). For a discussion of the concerns leading to adoption of this exception, see *Commerce Hearing*, *supra* note 44, at 12-18 (statement of Marc Rotenberg, Director, Electronic Privacy Info. Ctr.).

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, because 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)(1) 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.

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

---

139. *See* 17 U.S.C.A. § 1201(j).

140. *See, e.g.*, John Markoff, *Software Security Flaw Puts Shoppers on Internet at Risk*, N.Y. TIMES, Sept. 19, 1995, at A1.

141. *See* 17 U.S.C.A. § 1201(c)(4).

142. *See supra* note 136 (licensor whose self-help feature might be defeated by a licensee).

143. *See* 17 U.S.C.A. § 1204.

144. *See id.* § 1201(c)(1).

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 section.

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

The text of the DMCA and its legislative history clearly demonstrate 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 recognition that circumventions for fair use, free speech, and

145. Section 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. *Id.* § 1203(a).

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. Conversation with Julie E. Cohen (Jan. 1999).

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 rule 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 part has shown, if Congress had 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., enciphered text might be decoded 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, 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 privi-

147. *See* 17 U.S.C.A. § 1201(c)(1), (c)(4), discussed *supra* notes 99, 107, 113-116 and accompanying text. This same subsection indicates that it also does not intend to enlarge or diminish vicarious or contributory copyright infringement. *See id.* § 1201(c)(2).

148. *See id.* § 1201(a)(1)(B)-(D).

149. *See id.* § 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.

150. *See* Benkler, *supra* note 24, at 416 ("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 users 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" for fair use would be meaningful, given that most users would be unable to overcome technical protection systems without tools designed for that purpose).

leges),[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) 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 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 tool was, after all, "primarily designed ... for the purpose of circumventing protection afforded by a technological

152. *See* 17 U.S.C.A. § 1201(f)(2), (g)(4).

153. *See id.* § 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 § 1201(e) indicates that "this section does not prohibit any lawfully authorized investigative ... activity" of a government agent.

154. *See id.* § 1201(f)(2).

155. *See id.* § 1201(g)(4), (j)(4).

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

157. *See supra* note 114-116 and accompanying text.

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

measure that effectively protects a right of the copyright owner under this title in a work or a portion thereof."[159] 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,[160] a court might decide that this code should not be held to violate this law.[161]

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[king]" in this technology or "offer[ing it] for sale" which are the principal activities Congress meant to curb by enacting this part of DMCA.[162] 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 1985 *Vault v. Quaid*[163] case would fare under the DMCA anti-device provisions. Vault sued Quaid for contributory copyright infringement based on Quaid's development and sale of a program called Ramkey. Quaid's customers could use Ramkey to defeat Vault's Prolok copy-protection software (which Vault sold to other software developers to protect their own software from unauthorized copying). By spoofing Vault's copy-protect system,[164] Quaid's customers could make unauthorized copies of the third-party software protected by Vault's program.[165] Quaid successfully defended against the

159. *Id.* § 1201(b)(1).

160. *See* House Manager's Report, *supra* note 63, at 9-13.

161. Alternatively, the court could find only a technical or de minimis violation of the statute in this instance.

162. 17 U.S.C.A. § 1201(b)(1).

163. 775 F.2d 638 (5th Cir. 1985).

164. In essence, this and other "spoofing" software generally operate by emitting a signal which will be interpreted by the other firm's copy-protection software (or conceivably hardware) as an indication that the system is operating effectively.

165. Vault also claimed direct copyright infringement, trade secret misappropriation, and breach of contract. *See Vault*, 847 F.2d at 257-58.

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.[166]

Quaid would probably not run afoul of the access-device provision of section 1201(a)(2).[167] 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, because it would show a lack of wrongful intent. But would it save Quaid from civil liability?[168]

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 con-

166. *See id.* at 262 (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).

167. 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 § 1201(a)(2) inapplicable to the *Vault v. Quaid*-like controversies.

168. An interesting question is who could sue Quaid under § 1201(b)(1). The Clinton Administration's Green Paper on Intellectual Property and the National Information Infrastructure suggested that the maker of a protective technology, such as Vault, would not have standing to challenge the maker of circumvention technologies. *See* U.S. GOV'T WORKING GROUP ON INTELLECTUAL PROPERTY, GREEN PAPER ON INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 130 (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, *see infra* note 194 and accompanying text, in none of these lawsuits would the plaintiff have to demonstrate that any underlying act 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.A. § 1203(a) to facilitate its ability to obtain standing in such a suit were not heeded by Congress. *See Judiciary Hearing*, *supra* note 17, at 271-77 (statement of Mark S. Belinksy, Vice President, Copy Protection Group, Macrovision Corp.).

trol its work (in this case, a right to control illegal copying).[169] On the other hand, the DMCA recognizes that fair use-like circumventions should be lawful.[170] Backup copying is a specially privileged activity in the copyright statute.[171] Because 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 generally 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 the technically sophisticated will often need to develop a tool to accomplish a privileged circumvention; this would seem to put them at risk under a strict reading of section 1201(b)(1).[172]

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."[173] If what this subsection purports 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 they are certainly not constrained to do so.

Moreover, the major copyright industries that supported a broad ban on circumvention technologies would assert that courts should not construe the DMCA so narrowly. They would likely consider Quaid's argu-

---

169. *See* 17 U.S.C.A. § 1201(a)(2), (b)(1).

170. *See id.* § 1201(c)(1), discussed *supra* notes 99, 107, 113-116, 147 and accompanying text.

171. *See* 17 U.S.C. § 117 (1994).

172. Even they, of course, may have to manufacture a technology or provide a service to make backup copies, in apparent violation of section 1201's anti-device rules. *See* Benkler, *supra* note 24, at 416.

173. 17 U.S.C.A. § 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 163-166 and accompanying text.

ment 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.[174] 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.[175] 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 copyright owners are using to protect rights granted to them by copyright law.[176] According to 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.[177] Privacy advocates have raised concerns about the threat that processor identification systems pose for personal privacy on the Internet.[178] In response to these

---

174. *See Judiciary Hearing*, *supra* note 17, at 57 (statements of Hon. Bruce A. Lehman, Commissioner of Patents and Trademarks, Patent and Trademark Office).

175. *See Commerce Hearing*, *supra* note 44, at 54-58 (prepared statement of Steven J Metalitz on behalf of the Motion Picture Ass'n of America) (objecting to proposals that would require copyright owners to prove that circumvention or circumvention devices would cause infringement).

176. 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 15, app. 1 at 6. How, if at all, this might affect the scope of the DMCA's anti-device provisions remains to be seen.

177. *See* Peter H. Lewis, *Whoosh! The Next Pentium Chip Is On Its Way*, N.Y. TIMES ON THE WEB (Jan. 14, 1999) <http://www.nytimes.com/library/tech/99/01/circuits/-articles/12pete.html>.

178. *See* Jeri Clausing, *Privacy Groups Seek Recall of Intel Chip*, N.Y. TIMES ON THE WEB (Jan. 29, 1999) <http://www.nytimes.com/library/tech/99/01/cyber/articles/-29privacy.html>. 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 pre-

concerns, Intel announced its intent to ship these chips with the processor identity function "off."[179] Suppose, however, that Microsoft develops Windows 2000 as a "trusted system" technology[180] 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.[181] 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.[182] If a privacy advocacy group developed and distributed software to 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)?[183]

---

vent "piracy" of software has also been recognized. *See* Peter Wayner, *Debate on Intel Chip Misses Piracy Issue*, N.Y. TIMES ON THE WEB (Jan. 30, 1999) <http://www.nytimes.com/library/tech/99/01/cyber/articles/30chip.html>.

179. *See* Jeri Clausing, Intel Alters Plan Said to Undermine PC Users' Privacy, N.Y. Times, Jan. 26, 1999, at A1.

180. "Trusted system" is a term used to describe a computer and software system constructed to make it impossible (or at least very difficult) to make unauthorized copies or uses of legally protected works. *See* 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).

181. This is no mere conjecture. Microsoft is reportedly intending to deploy trusted system software with the next version of Windows. *See* Jason Chicola et al., Digital Rights Architectures for Intellectual Property Protection 99 (1998), paper prepared for *Ethics and Law on the Electronic Frontier*, Massachusetts Institute of Technology, *available at* <http://swissnet.ai.mit.edu/6805/student-papers/fall98-papers/trusted-systems/trustsys.doc> (MS Word document). 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.

182. 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); Symposium, *Intellectual Property and Contract Law for the Information Age: The Impact of Article 2B of the Uniform Commercial Code on the Future of Information and Commerce*, 87 CALIF. L. REV. 1 (1999).

183. 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

Under a very strict interpretation of section 1201(b)(1), either act might be viewed as illegal.[184] 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.[185] 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 the 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.[186] 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.[187] 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 Administration officials and 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.[188] It sought only to outlaw technologies whose "primary purpose or effect" was

works under § 1201. If so, it would seem that a hardware device which disables the Processor Serial Number could be 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.shtml>.

184. Posting information on the website might be seen as providing a service to the circumventors.

185. *See* 17 U.S.C.A. § 1201(i) (West Supp. 1999). This provision is extremely complicated and would seem to be very narrow. It is not clear it would apply to the Microsoft example.

186. *See supra* note 93 and accompanying text and *infra* note 231.

187. *See* Benkler, *supra* note 24, at 416.

188. *See* White Paper, *supra* note 15, at 230-36.

to enable the circumvention of technical protection measures.[189] 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 (due to the unavailability of circumvention devices), 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.[190] 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.[191]

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 effectively be nullified by section 1201(b)(1), which arguably broadly bans technologies necessary to accomplish such circumventions.

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.[192] Yet, the

189. *See id.*, app. 1 at 6.

190. *See supra* note 86.

191. Professor Benkler likens this strategy to banning VCRs in order to stop home taping. *See* Benkler, *supra* note 24, at 416. 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.A. § 1201(k) (West Supp. 1999).

192. *See Judiciary Hearing*, *supra* note 17, at 212-16 (statement of Gail Markels, General Counsel and Senior Vice President, Interactive Digital Software Ass'n) (relying on example of circumvention device with no legitimate purpose that had been used to pirate games); *id.* at 273-77 (prepared statement of Mark Belinsky on behalf of Macrovi-

anti-device provisions adopted by Congress are far broader than this, providing a basis to challenge an unacceptably wide range of 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.[193]

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.[194] 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

---

sion Corp.) (emphasizing the need to outlaw pirate devices). *See also NII Copyright Protection Act of 1995 (Part II): Hearings on H.R. 2441 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 104th Cong. 23 (1996) (prepared statement of Jack Valenti, President and CEO, Motion Picture Ass'n of America) ("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.").

193. Some commentators even perceive the anti-device rules of § 1201 as threatening the distribution of many widely used editing and related software tools. *See* Peter Wayner, *The Copyright Boomerang*, SALON MAGAZINE (Nov. 20, 1998) <http://www.salonmagazine.com/21st/feature/1998/11/20feature.html> (considering whether "cutting and pasting" will be rendered unlawful).

194. *See* Complaint, Sony Computer Entertainment, Inc. v. Connectix Corp., Civ., No. 99-0390 (N.D. Cal., filed Jan. 27, 1999) [hereinafter Sony Complaint]. For a discussion of this lawsuit, see Band & Isshiki, *supra* note 65.

the games.[195] The plaintiff did not allege and 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. 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,[196] they are likely to have harmful effects on competition and innovation in the high technology sector. This is not good news for the digital economy.

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

The Clinton Administration did not recommend or support inclusion of any provision in the WIPO treaty implementation legislation to assess the impact of the DMCA's anti-circumvention norms.[197] 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.[198] 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

---

195. *See* Sony Complaint, *supra* note 194, at 7-8. This lawsuit is particularly disturbing because the software at issue was named "Best of Show" at Macworld Expo shortly before the lawsuit was filed. *See Best of Show*, MACWORLD ONLINE (visited Apr. 21, 1999) <http://macworld.zdnet.com/expo/report/bestofshow.html>.

196. A predictable, minimalist, consistent, and simple anti-device norm might outlaw the manufacture and distribution of technologies intended to facilitate copyright infringement or of technologies with limited legitimate uses.

197. *See* H.R. 2281, 105th Cong. (1997) (as originally introduced into Congress on July 29, 1997); *Judiciary Hearing*, *supra* note 17, at 34-42 (statement of Bruce Lehman) (endorsing legislation but not asking for a study provision).

198. *See Judiciary Hearing*, *supra* note 17, at 148-56 (statement of Robert L. Oakley); *id.* at 64-68 (statement of M.R.C. Greenwood).

harm to copyright owners.[199] 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 digital economy markets, namely, the proposal to create a new form of legal protection for the contents of databases.[200] 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.[201]

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.[202] 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-

---

199. One of the few concrete examples of a device claimed to have contributed to international piracy was that offered in *Judiciary Hearing*, *supra* note 17, at 213-216 (statement of Gail Markels) (discussing "Game Doctor" said to have been used to pirate game software in Hong Kong and Taiwan).

200. *See* Letter from Andrew Pincus, General Counsel of the U.S. Dep't of Commerce, to Sen. Patrick Leahy 3 (Aug. 4, 1998) (on file with author) [hereinafter Pincus Letter]. After the House passed the Collections of Information Antipiracy Act, H.R. 2652, 105th Cong. (1998), Mr. Pincus wrote to Senator Leahy to express the Administration's reservations about the wisdom of this bill and about its constitutionality. *See* Pincus Letter, *supra*, at 1.

201. Pincus Letter, *supra* note 200, 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.*

202. *See* 145 CONG. REC. S322 (daily ed. Jan. 19, 1999) (provision entitled "Report to Congress," from one of three potential database bills referred to by Sen. Hatch).

circumvention regulations.[203] 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,[204] the House Commerce Committee decided that there should be a two-year moratorium on enforcement of the act-of-circumvention provision.[205] 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.[206]

The Commerce Committee's insistence on the moratorium and an impact study 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.[207] 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.[208] Subsection (B) goes on to provide the statutory basis for granting such an exemption to the classes of works or users determined by the Librarian to be adversely affected by the anti-circumvention norm.[209] The DMCA calls for the Librarian's first study to be completed before the anti-circumvention moratorium ends.[210]

---

203. *See* 17 U.S.C.A. § 1201(a)(1)(B)-(D) (West Supp. 1999). Section 1201 also contains a provision for studying the impact of the encryption research provision. *Id.* § 1201(f)(5).

204. *See supra* note 117 and accompanying text.

205. *See Commerce Panel Clears Digital Copyright Bill With Further Concessions On Fair Use*, 56 BNA PAT., TRADEMARK & COPYRIGHT J. 326, 326 (1998).

206. *See id.* As Professor 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. *See* Benkler, *supra* note 24, at 428.

207. 17 U.S.C.A. § 1201(a)(1)(A) (West Supp. 1999).

208. The first study is to be completed two years after the date of DMCA's enactment. *See* 17 U.S.C.A. § 1201(a)(1)(A) (West Supp. 1999). Follow-on studies are to be conducted every three years thereafter. *See id.* § 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 63, at 6-7.

209. *See* 17 U.S.C.A. § 1201(a)(1)(B) (West Supp. 1999). It appears that any moratorium resulting from such a determination will last for three years. *Id.* § 1201(a)(1)(D). The rulemaking procedure set forth in § 1201(a)(1)(B)-(D) may, however, be unconstitu-

The DMCA directs the Librarian of Congress to consider four factors in carrying out this study:

> (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."[211]

The Librarian has authority to consider "such other factors as the Librarian considers appropriate."[212] The DMCA is quite clear, however, that the Librarian's determinations cannot be asserted as a defense to an anti-device claim.[213] 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 could accomplish the act without a device, once again raising the specter 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.[214] 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,[215] they fall far short of the periodic review and reporting process appropriate to the unprecedented nature of the anti-circumvention regulations.[216] To

---

tional because the Librarian of Congress is not an executive branch official. *See* Band & Isshiki, *supra* note 65, at 7.

210. *See* 17 U.S.C.A. § 1201(a)(1)(A) (West Supp. 1999).

211. *Id.* § 1201(a)(1)(C). 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.* § 1201(g)(5).

212. *Id.* § 1201(a)(1)(C).

213. *See id.* § 1201(a)(1)(E).

214. *See* Benkler, *supra* note 24, at 428.

215. 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..

216. 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

limit an assessment of the circumvention ban to a narrow range of possible effects would ignore the wider swath of harm the provision may do.[217] Besides, the device ban is the true heart of the anti-circumvention provisions of the DMCA. It is integrally interrelated with the circumvention activity ban.[218] To assess the act-of-circumvention ban without considering the 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.[219] 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.[220] 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.[221]

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

---

studies of the impact of anti-circumvention rules "upon the recommendation of the Register of Copyrights." *Id.* § 1201(a)(1)(C). The Register, in turn, is supposed to consult with an official from the Department of Commerce before recommending a study. *See id.* It has been a long time since the Register 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, because none of the Librarian's findings last for more 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.

217. See *supra* note 136-140 and accompanying text for examples of legitimate circumvention activities unlikely to be captured by the scope of the intended studies by the Librarian.

218. *See supra* notes 24 and accompanying text. *See also* Benkler, *supra* note 24, at 416.

219. *See supra* notes 28-36 and accompanying text.

220. *See* 17 U.S.C.A. § 1201 (a)(1)(C) (West Supp. 1999) (setting forth factors); *see also* Benkler, *supra* note 24, at 420 ("[E]nforcement of the anti-device provision is unconstitutional unless and until the Librarian makes a determination that no non-infringing uses will be adversely affected by utilization of technological protection measures.").

221. See *supra* notes 136-140 and accompanying text for examples of other potential deleterious effects.

proof needed to maintain an action for anti-circumvention violations,[222] along with the generous remedies the Act provides,[223] may prove to be a magnet for firms seeking to challenge acts of circumvention or devices that might, for example, concern trade secrecy or computer hacking matters.[224] 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,[225] 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 Part VI has shown, section 1201 is so ambiguous and broad that it may wreak considerable havoc in the information technology field, harming competition and innovation in this important sector. For these reasons, a broad regular review of the anti-circumvention rules should be undertaken.

VIII. 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*.[226] 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 promises to substantially benefit the U.S. digital economy industries.

In most respects, the legislation implementing the WIPO Copyright Treaty in U.S. law also conforms to Framework principles.[227] The anti-circumvention provisions of the DMCA, however, do not. They are unpredictable, overbroad, inconsistent, and complex. The many flaws in this

---

222. *See supra* notes 174-176, 193-195 and accompanying text.

223. *See* 17 U.S.C.A. § 1203(b) (West Supp. 1999) (civil remedy provision).

224. This potential was recognized in the Congressional debate over the anti-circumvention rules. *See* 144 CONG. REC., H7096 (daily ed. Aug. 4, 1998) (remarks of Rep. Goodblatte). Although Rep. Goodblatte 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 § 1201.

225. *See* 17 U.S.C. § 102 (1994) (copyright protection subsists in all original works of authorship that have been fixed in a tangible medium of expression).

226. *See* FRAMEWORK, *supra* note 1, at 3.

227. *See supra* notes 70-72 and accompanying text.

legislation are likely to be harmful to innovation and competition in the digital economy sector, and harmful to the public's broader interests in being able to make fair and other noninfringing uses of copyrighted works. If these regulations are not as maximalist as those 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 have been 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.[228] The diplomatic conference had the good sense to adopt only a general norm on circumvention, leaving nations free to implement this norm in their own way.[229] 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 overbroad rules in the DMCA.

This article has demonstrated that the DMCA's ban on the act of circumventing 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.[230] 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 principal intent of Congress was to ban the development and deployment of "black boxes" that promote and enable piracy of copyrighted works.[231] However, the ban is far broader than this and threatens to bring about a flood of liti-

228. *See supra* notes 51, 87-89 and accompanying text.
229. *See supra* note 51 and accompanying text.
230. *See supra* notes 136-146 and accompanying text.
231. *See supra* notes 93 and accompanying text.

gation 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.[232] 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.[233] 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 their impact as a whole.[234] 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 interferes with the ability of certain classes of users to make noninfringing uses of certain classes of copyrighted works.[235] This provision is too narrow in at least two respects. One is that it does not perceive the potential impact of the device bans on the ability of users to make noninfringing uses of copyrighted works. The Librarian of Congress can and should consider this as well.[236] A second is that the DMCA's study provision does not recognize other kinds of potential harm that the anti-circumvention provisions may do to competition and innovation in the information technology sector.[237] 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 copyrighted works are being distributed with technical pro-

232. *See supra* notes 194-195 and accompanying text.
233. *See supra* notes 150-151 and accompanying text.
234. *See supra* notes 215-225 and accompanying text.
235. *See* 17 U.S.C.A. § 1201(a)(1)(B).
236. *See supra* notes 220 and accompanying text.
237. *See supra* notes 217 and accompanying text.

tection systems built in.[238] Much research and development work is, however, underway to develop such systems.[239] 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.[240]

One factor that will significantly affect how widely technical protection systems will be deployed and how tightly they will restrict uses of copyrighted works is how consumers will react to them.[241] 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.[242]

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

---

238. *See* COMPUTER SCIENCE AND TELECOMMS. BD., NATIONAL ACADEMY OF SCIENCES, INTELLECTUAL PROPERTY RIGHTS AND THE EMERGING DIGITAL ECONOMY (forthcoming 1999).

239. *See* Eric Schlachter, *The Intellectual Property Renaissance in Cyberspace: Why Copyright Law Could Be Unimportant on the Internet*, 12 BERKELEY TECH. L.J. 15, 38-45 (discussing various kinds of systems).

240. *See* Charles Clark, *The Publisher in the Digital World*, *in* INTELLECTUAL PROPERTY RIGHTS AND NEW TECHNOLOGIES: PROCEEDINGS OF THE KNOWRIGHT'95 CONFERENCE 85 (Klaus Braunstein & Peter Paul Sint eds., 1995). *See also* White Paper, *supra* note 15, at 177-90 (foreseeing wide deployment).

241. 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).

242. *Id.* at 98.

of the non-rival nature of information, prevailing economic theory would suggest that we are as likely to lose as gain productivity from this technological change."[243] In addition, if consumers won't buy tightly restricted copies, copyright owners may end up worse off than before.[244]

Competition among information providers may also affect the successful deployment of technical protection systems. If one information provider tightly locks up his content, a competing provider may see a business opportunity in supplying a less tightly restricted copy to customers who might otherwise buy from the first provider.[245] A competitive alternative to tight technical controls may well be to adopt one of the several strategies that Shapiro and Varian discuss to show how content providers can take advantage of the opportunities presented by digital technologies, rather than being overwhelmed by the risks.[246] There are, they say, many other good business models out there waiting to be invented by creative content providers.[247]

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. Benkler, *supra* note 24, at 424.

244. *See* Branko Geravac et al., *Electronic Commerce and Intellectual Property—Protect Revenues, Not Bits*, 2 IMA INTELL. PROP. PROC. 111 (1996).

245. This, in essence, is 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.

246. *See* SHAPIRO & VARIAN, *supra* note 241, ch. 4.

247. *See id.* at 84. Some of these business models may themselves be subject to intellectual property protection. *See, e.g.*, Robert P. Merges, *As Many as Six Impossible Patents Before Breakfast: Property Rights for Business Concepts*, 14 BERKELEY TECH. L.J. 577 (1999).