Preliminary Draft 2/14/96

TECHNOLOGICAL PROTECTION FOR COPYRIGHTED WORKS

by
Pamela Samuelson*

"Something there is that doesn't love a wall."[1]

I. INTRODUCTION

Digital technology poses a serious challenge for copyright owners because works in digital form are vulnerable to uncontrolled replication and dissemination in networked environments.[2] Digital technology is, however, not just part of the problem; it may also be part of the solution.[3] Developments in digital technology open up new opportunities for publishers to control reproductions and disseminations of copies of copyrighted works, to detect the existence of unauthorized reproductions, adaptations, or disseminations, to trace the whereabouts of unauthorized reproductions or disseminations, and to monitor usages of works in ways that were impossible or

---

* Professor of Law, University of Pittsburgh Law School. This paper has been prepared for the Thrower Symposium at Emory Law School, February 22, 1996, and is slated for publication in 45 EMORY L.J. (forthcoming 1996). Thanks go to my research assistant Benjamin Black for outstanding work in connection with preparation of the article. Thanks are also offered to Robert J. Glushko for his insightful comments on an earlier draft of this article.

1 Robert Frost, The Mending Wall, in THE NEW OXFORD BOOK OF AMERICAN VERSE 395-96 (R. Elman, ed. 1976).

2 This vulnerability is said to be a factor inhibiting the growth of markets for digital information products on the "information superhighway." Some publishers are unwilling to make content available on this highway unless they have assurance that protection of some kind is available to avert market-destructive appropriations of this content, as might occur if the first purchaser of the content posted it on publicly accessible bulletin board systems, enabling members of the public to get access to the content without payment of a fee to its publisher. See, e.g., NATIONAL INFORMATION INFRASTRUCTURE TASK FORCE, REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE (Sept. 1995) (cited hereinafter as "White Paper"); John Perry Barlow, The New Economy of Ideas, WIRED 2.04 (March 1994).

3 As one publisher has aptly put it, "the answer to the machine is the machine." Charles Clark, "The Answer to the Machine Is the Machine," PROCEEDINGS OF KNOWRIGHT '95 (1995). See also CHRISTOPHER BURNS, COPYRIGHT MANAGEMENT AND THE NII: REPORT TO THE ENABLING TECHNOLOGIES COMMITTEE OF THE ASSOCIATION OF AMERICAN PUBLISHERS, May 31, 1995, and Mark Stefik, Letting Loose the Light: Igniting Commerce in Electronic Publication (March 7, 1995).

infeasible in relation to printed copies.[4] Technology holds much promise as a way to relieve copyright law of the burden of attempting to regulate a wide range of activities by users of digital information products, most of which, by virtue of the highly decentralized nature of existing digital networks, would be difficult for the law to regulate effectively. Very considerable investments are currently being made to develop or refine technological means for protecting copyrighted material in digital form.[5]

As bright as are the prospects for technological protection for copyrighted works, there are some worrisome aspects of technological protection as well. The principal concern of publishers is that what one technology can do, another technology may well be able to undo through clever circumvention or bypass techniques. Although court decisions allow copyright owners to control sale of technologies that have no substantial use other than to enable copyright infringement,[6] some publishers regard this rule to be inadequate to protect their works against technological piracy.[7] They support legislation that would make it illegal to sell or distribute products or offer or provide services, "the primary purpose or effect of which is to avoid, bypass, remove, deactivate or otherwise circumvent, without the authority of the copyright owner or the law, any process, treatment, mechanism, or system which prevents or inhibits the violation of any of the exclusive rights of the copyright owner under section 106."[8] A provision of this sort is under active consideration in the U.S. Congress.[9] The United States is urging inclusion of a very similar provision in an international treaty to supplement the Berne Convention.[10]

As legitimate as are publisher concerns about circumvention technology, this article will argue that the anti-circumvention proposal currently under consideration is overbroad and is in need of substantial refinement. It will also explore the implications of the use of copyright law as a means to regulate technologies, and in particular, as a means of controlling public access to information that may be embedded in information products. The anti-circumvention provision recommended

---

[4] See, e.g., PROCEEDINGS ON TECHNOLOGICAL STRATEGIES FOR PROTECTING INTELLECTUAL PROPERTY IN THE NETWORKED MULTIMEDIA ENVIRONMENT, 1 J. INTERACTIVE MULTIMEDIA ASS'N 1 (Jan. 1994) (cited hereinafter as "IMA Proceedings").

[5] Id.

[6] Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984). See infra notes -- and accompanying text.

[7] See, e.g., NATIONAL INFORMATION INFRASTRUCTURE TASK FORCE, WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS, GREEN PAPER ON INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE (Prelim. Draft July 1994) (cited hereinafter as "Green Paper") at 126.

[8] NII Copyright Act §4, White Paper, supra note 2, Appendix 1 at 6.

[9] See H.R. 2441, 104th Cong., 1st Sess. (1995); S. 1284, 104th Cong., 1st Sess. (1995).

[10] PROPOSALS SUBMITTED BY THE UNITED STATES OF AMERICA TO COMMITTEE OF EXPERTS ON A POSSIBLE PROTOCOL TO THE BERNE CONVENTION, SIXTH SESSION, GENEVA, Feb. 1-9, 1996 (cited hereinafter as "U.S. Submission").

in the Clinton Administration's White Paper on Intellectual Property and the National Information Infrastructure (NII) [11] has potential to open up a brave new world for copyright law, one that would recast it as a law to protect trade secrets or other private information, to undermine public access to public domain information, to promote public or private censorship of exchanges of information, and possibly to impede law enforcement activities. Before leaping into this brave new world for copyright, we should consider whether there are sometimes reasons not to love the walls that some will build with technological protection. Some sober reflection is needed about whether the laudable purposes sought to be accomplished by the anti-circumvention provision might be better served by a more narrowly drawn provision. Also needed are some imaginative ideas about how the historical balance among author, publisher, and user interests in copyright law might be maintained in digital networked environments.

II. AN HISTORICAL PERSPECTIVE ON COPYRIGHT AS A FORM OF REGULATION OF TECHNOLOGY

Prior to the invention of the printing press, there was no copyright law. This did not necessarily mean that texts were freely appropriable.[12] Among the factors inhibiting the free appropriation of texts in that era was a substantial lack of literacy skills and of technologies needed to engage in copying (e.g., vellum and writing implements), but also the need for access and permission to make copies that could only be granted by the owners of physical embodiments of the texts. During the Middle Ages, the Catholic Church often limited such access and permission to those deemed by the Church to be safe as guardians of this content.[13] Permission to access and copy texts was likely to be conditioned on an agreement to abide by certain rules in relation to the texts or copies of them.[14]

The first copyright rules in England were, to a considerable degree, a form of regulation of printing and of printers. English monarchs relegated to the Stationers' Company, an association of printers, bookbinders, booksellers, and the like, the right to control the printing and distribution of books, in exchange for which members of

---

[11] White Paper, supra note --.

[12] See, e.g., ROBERT A. GORMAN AND JANE C. GINSBURG, COPYRIGHT IN THE NINETIES 1 (1993), reporting that an Irish King had resolved a dispute over a manuscript with the maxim "To every cow, her calf."

[13] This conception of the library is nicely illustrated in UMBERTO ECO, THE NAME OF THE ROSE (1989). See generally MARK ROSE, AUTHORS AND OWNERS: THE INVENTION OF COPYRIGHT (1993).

[14] Id. This history is worth noting because in some measure, digital technology is taking us back to the Middle Ages, in that many online information providers are conditioning rights to access and use their content on agreement to abide by specific terms, such as an agreement not to reuse the content for particular purposes. Lawyers and law students are, for example, with Westlaw's aggressive assertion of rights to control reuse of electronic versions of judicial opinions and statutes that are downloaded from its system.

the Stationers' Company agreed not to publish seditious or heretical materials.[15] The printing of unauthorized materials, or of authorized materials by unauthorized printers, was punishable by decrees of the Star Chamber and/or by Stationers' Company enforcement proceedings.[16] Rules of the Stationers' Company enabled members to obtain exclusive rights to publish particular books by being the first to inscribe their claims of "copyright" in the Company's register. Stationers claimed copyright in these works by virtue of investments made in acquiring manuscripts and printing their texts in books. The printer's "copyright" was claimed in perpetuity, unhampered by any requirement of "originality" in the text or of relatively recent authorship of the work.[17]

Members of the Stationers' Company would have preferred continuation of their copyright system forever. However, over time, a combination of circumstances--complaints by authors that printers were unfairly appropriating their works, by unlicensed printers about the unfairness of their exclusion from competition with licensed stationers, and by the public about exorbitant prices for books and the silencing of dissenting views by reason of censorship the stationers' copyright regime brought about--led to the demise of this system.

The first modern copyright law, namely, the Statute of Anne in 1710, brought about several changes: (1) copyright was now initally vested in authors, rather than publishers; (2) the rationale given for the grant of rights to authors was to encourage learned men to compose useful books and make them available in order to promote learning more generally; (3) as a consequence, copyrights were now available primarily to newly authored works; (4) as a further consequence, copyright was no longer perpetual in duration, but lasted for only fourteen years from the date of first publication of a work;[18] and (5) in the event that complaints arose as regards the prices charged for books, a procedure was established by which to address such complaints.[19]

The Statute of Anne regulated printing technology by granting authors exclusive rights to print, reprint and vend books embodying their works. However, its significance goes beyond this. By rejecting the stationers' copyright system, which in conjunction with the Licensing Act provisions, had restricted entry into the printing and bookbinding businesses, the English Parliament adopted utilitarian incentive and anti-monopoly principles in copyright law. It also endorsed promotion of learning as a

---

[15] See, e.g., L. RAY PATTERSON, COPYRIGHT IN HISTORICAL PERSPECTIVE (1968).

[16] Id.

[17] Id. Directories of information and works of ancient authors could be copyrighted under the Stationers' copyright system. This history too is worth relating because of the potential new technologies may present for getting what may amount to perpetual exclusive rights in information or other matter considered uncopyrightable under existing intellectual property laws.

[18] An author could renew his copyright if he was living at the time his first copyright term was about to expire.

[19] See, e.g., Gorman & Ginsburg, supra note --, at 2-4 (describing contents of the act) ; Rose, supra note --, at 42-48 (discussing its legislative history).

central purpose of copyright, embracing Enlightenment principles that, over time, came to be reflected in the first amendment to the U.S. Constitution. U.S. antitrust and anti-censorship traditions, in part, trace their origins to this history.[20]

While copyright laws in England and the U.S., as well as kindred laws in other jurisdictions, continue to regulate the printing and reprinting of books, they have expanded considerably the rights of authors (and their assigns) to control uses of technologies that can be used to reproduce or perform copyrighted works.[21] Until relatively recently, however, the costs of reprography and performance technologies were sufficiently high, and their uses were sufficiently public, that there was relatively little danger that infringement on a commercially significant scale would arise from individual user activities.

The late twentieth century has witnessed the advent of a number of relatively low-cost reprography technologies--photocopying machines, tape recorders, and computers, among them--that can be used by ordinary people to make inexpensive copies of copyrighted works that are far less public in character.[22] These technologies have shifted the effective balance of power as among authors, publishers and users in favor of users. As a consequence of the widespread availability of these reprography technologies and few restrictions on their use, ordinary users have come to believe that most, if not all, private, noncommercial copying of copyrighted works is not only beyond the power of copyright owners to control, but beyond their legal rights as well.[23]

While some authors and publishers might concede that private noncommercial copying is largely beyond their power to control, they are less willing to concede the point about their legal authority.[24] Notwithstanding some notable losses in lawsuits challenging some private uses of reprography technologies in the 1970's and 1980's,[25] publisher challenges to research and educational use copying have met with greater

---

[20] See, e.g., L. Ray Patterson, Free Speech, Copyright, and Fair Use, 40 VAND. L. REV. 1 (1987) (discussing free speech implications) and L. Ray Patterson and Craig Joyce, Monopolizing the Law: The Scope of Copyright Protection for Law Reports and Statutory Compilations, 36 UCLA L. REV. 719 (1989) (discussing anti-monopoly implications).

[21] The Copyright Act of 1976 identifies protectable works of authorship to include pictorial, sculptural and graphic works, motion pictures and other audiovisual works, choreographic works and pantomimes, among others. 17 U.S.C. §102(a).

[22] Congressional concern about these reprographies led it to create a Commission to study the copyright implications of these technologies. See NATIONAL COMMISSION ON NEW TECHNOLOGICAL USES OF COPYRIGHTED WORKS, FINAL REPORT (1978).

[23] See, e.g., OFFICE OF TECHNOLOGY ASSESSMENT, INTELLECTUAL PROPERTY RIGHTS IN AN AGE OF ELECTRONICS AND INFORMATION (1986).

[24] See, e.g., PAUL GOLDSTEIN, COPYRIGHT'S HIGHWAY (1995) (giving examples).

[25] See, e.g., Williams & Wilkins Co. v. United States, 487 F.2d 1345 (Ct. Cl. 1973), aff'd by an equally divided Court, 420 U.S. 376 (1975) (library photocopying of medical research articles held fair use); Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984) (videotaping for time-shifting purposes held fair use).

success in the 1990's.[26] However, the hearts and minds of the populace have not been won over to the strong protectionist position favored by some publishers.

Much effort is currently being devoted to developing ways to use technology to shift the balance of power back in the direction of greater publisher control. Several steps are contemplated to accomplish this balance shifting: first, many publishers plan to use technological means, such as encryption or digital envelopes, to protect content against unauthorized copying;[27] second, many support enactment of the broad anti-circumvention provision mentioned above;[28] and third, some publishers are planning to propose that manufacturers of reprography technologies be required to embed secure processors to prevent unauthorized access to or copying of copyrighted works in their technologies.[29] This proposal is already under serious consideration in the European Union,[30] and is favored by major copyright industries.[31]

The policy climate in which these initiatives are taking place is somewhat less hospitable to their general tenor than many publishers would care to admit. Courts have been far less sympathetic to expansionist interpretations of copyright law as a means of regulating technology; they have generally been reluctant to allow copyright law to be used to regulate technologies beyond that which has been explicitly

---

[26] See, e.g, Basic Books, Inc. v. Kinko's Graphics Corp., 758 F. Supp. 1522 (S.D.N.Y. 1991)(photocopying of coursepacks consisting largely of excerpts of copyrighted works held unfair); American Geophysical Union v. Texaco, Inc., 37 F.3d 881 (2d Cir. 1994), amended and superceded, 60 F.3d 913 (2d Cir. 1995) (copying of individual research articles from journals held unfair). But see Princeton University v. Michigan Document Services, 1996 U.S. App. LEXIS 1919 (6th Cir. 2/12/96) (coursepack photocopying held fair use).

[27] See, e.g., Burns, supra note --.

[28] See supra note --.

[29] Intel Corp. is reportedly working on the development of secure processors that will not operate if digital information about a copy does not contain an authorization code.

[30] See, e.g., COMMISSION OF THE EUROPEAN COMMUNITIES, GREEN PAPER ON COPYRIGHT AND RELATED RIGHTS IN THE INFORMATION SOCIETY, COM(95) 382 final (July 19, 1995).

[31] This last proposal is not mentioned in the Clinton Administration's White Paper. Given that uninhibited access to "insecure" reprography technology is widespread in the U.S., it may be strategically wise to win the anti-circumvention battle first, and undertake on the secure processor initiative later. The only hint that the White Paper gives about developments of this sort is in a footnote indicating support for equipment manufacturers and copyright industry negotiations about more secure technologies. White Paper, supra note --, at 232, n. 568.

authorized by Congress.[32] The decisions discussed below illustrate this historical reluctance.[33]

A. *Sony v. Universal*

In Sony Corp. of America v. Universal City Studios, Inc.,[34] the U.S. Supreme Court overturned a Ninth Circuit Court of Appeals ruling that Sony was liable for contributory infringement because it sold video tape recording (VTR) machines knowing that consumers would use these machines to make infringing copies of copyrighted works.[35] Universal City Studios and Walt Disney brought the action because they feared that home recordings of their movies would undermine theatre exhibitions and other revenue generating events. They claimed to have standing to sue because works in which they held copyright were among the programs that many consumers were using VTRs to record off broadcast television.[36] There was evidence in the case that the principal use to which consumers used VTRs at the time of this litigation was for "time-shifting" purposes,[37] i.e., the use of Betamax machines to record programs off the air in order to watch them at a later time. Consumers typically taped over previous recordings each time they needed to time-shift. The Ninth Circuit rejected arguments that Congress had intended to exempt private home copying of copyrighted works[38] and that time-shift copying was fair use.[39]

Various factors converged to persuade a majority of the Supreme Court that Sony should not be liable for contributory infringement. There being no contributory infringement provision in the copyright statute,[40] the Court considered whether to borrow the patent "staple item of commerce" rule which denies patent owners the right

---

[32] This is not to say that there have been no cases in which copyright liability has been found for distribution of technologies beyond explicit Congressional intent. See, e.g., Midway Mfg. Co. v. Artic Int'l, Inc., 704 F.2d 1009 (7th Cir.), cert. denied, 464 U.S. 823 (1983) (program that speeded up play of videogame held to infringe derivative work right); In re Certain Personal Computers, 224 U.S.P.Q.2d (BNA) 270 (U.S. Int'l Trade Comm'n 1984) (blocking importation of chips capable of noninfringing uses).

[33] These decisions are largely ignored in the White Paper. They are among the decisions that may be modified, if not overruled, if the anti-circumvention provision proposed in the White Paper is adopted. See infra notes -- and accompanying text.

[34] 464 U.S. 417 (1984).

[35] Universal City Studios, Inc. v. Sony Corp. of America, 480 F. Supp. 429 (S.D. Cal. 1979), rev'd 659 F.2d 963 (9th Cir. 1981), rev'd sub nom. Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984).

[36] Sony, 480 F. Supp. at 433-36.

[37] Id. at 438-39. Both parties had done surveys about uses of VTR's which showed this, though they differed somewhat about how high the proportion of time-shifting was.

[38] Sony, 659 F.2d at 965-69.

[39] Id. at 969-74.

[40] Sony, 464 U.S. at 434.

to control sales of products that are suitable for noninfringing uses[41] or a more trademark-like rule which would have imposed liability upon vendors who sold products knowing that they would be used for infringing purposes.[42] Citing "the historic kinship between patent law and copyright law"[43] and the public interest in access to technologies that have noninfringing uses,[44] the U.S. Supreme Court opted for the patent-like rule. As long as a technology was capable of substantial noninfringing uses,[45] the Court decided that its use could not be regulated by copyright owners.

Among the noninfringing uses of VTRs were copying uncopyrighted programs off-the-air or copying programs whose copyrights were owned by firms having no objection to time-shift copying.[46] The Court also decided that private noncommercial copying of copyrighted works, such as use of VTR's to record programs for time-shifting purposes, should be regarded as presumptively fair. This presumption of fairness would only be overcome if plaintiffs produced proof of some meaningful likelihood of harm from the use.[47] "[A] use that has no demonstrable effect upon the potential market for, or the value of, the copyrighted work need not be prohibited in order to protect the author's incentive to create. The prohibition of such noncommercial uses would merely inhibit access to ideas without any countervailing benefit."[48]

Another factor affecting the Court's view of the case was its doubts about the standing of Universal and Disney to maintain the lawsuit against Sony. Several times in the opinion the Court expressed this concern. At one point, the Court said: "[T]his is not a class action on behalf of all copyright owners who license their works for television broadcast, and respondents have no right to invoke whatever rights other copyright holders may have to bring infringement actions based on Betamax copying of their works."[49] Elsewhere, the Court observed that should Universal and Disney

---

[41] "Whoever sells a component of a patented machine, manufacture, combination or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple item of commerce suitable for substantial noninfringing use, shall be liable as a contributory infringer." 35 U.S.C. §271(c). See, e.g., Dawson Chemical Co. v. Rohm & Haas Co., 448 U.S. 176 (1980) (contributory infringement to sell an unpatented chemical whose only substantial use was in the practice of a patented process).

[42] Sony, 464 U.S. at 439, n.19. See, e.g., Inwood Labs., Inc. v. Ives Labs., Inc. 456 U.S. 844, 854-55 (1982) (discussing trademark contributory infringement standards).

[43] Id. at 439.

[44] Id. at 440-42.

[45] Id. at 442.

[46] Id. at 443-47

[47] Id. at 449.

[48] Id. at 450-51. The White Paper characterizes the Supreme Court's decision in Sony as resting on the failure of Universal and Disney to establish a licensing system for VTR recordings.

[49] Id. at 434.

prevail in the lawsuit, it would frustrate not only consumer interests in using VTR's but also the interests of copyright owners who wanted consumers to use these machines for time-shifting purpose as a way to enlarge audiences for their programs upon which advertising revenues for television viewing are based.[50] The Court also characterized as "extraordinary" the claim that "the Copyright Act confers upon all copyright owners collectively, much less the two respondents in this case, the exclusive right to distribute VTR's simply because they may be used to infringe copyrights."[51] In the absence of clear directions from Congress, the Court thought that the exclusive rights provisions of copyright law should not be construed in this manner.[52]

B. *Vault v. Quaid*

Vault developed a software-based copy-protection system called Prolok intended for sale to other software companies who would use Prolok to protect their software products before selling the protected versions of them to consumers. Quaid developed Ramkey, a software product that could be used to undo Vault's copy-protection system. Vault sued Quaid for direct and contributory copyright infringement.[53]

The direct infringement claim chiefly focused on copying of Vault's software that Quaid had done in order to learn how the copy-protection system worked so that Quaid could develop a technique to circumvent the system. Quaid did this analysis by means of "black-box testing," that is, by loading the Vault program onto its computers and testing it under various conditions to see what it would do, from which Quaid inferred some details of the internal design of the program.[54] Vault insisted that copying a program onto a computer in order to engage in such reverse analysis was copying beyond terms permitted by its shrink-wrap license and by copyright law. In Vault's view, the law and the license only authorized consumers to make copies necessary to use the program for its intended purpose as a copy-protection system.[55] The Court of Appeals found this argument unpersuasive.[56]

---

[50] Id. at 443.

[51] Id. at 441, n.21.

[52] Id. at 431, 457.

[53] Vault Corp. v. Quaid Software, Inc., 655 F. Supp. 750 (E.D. La. 19870, aff'd, 847 F.2d 255 (5th Cir. 1988). There were also breach of contract claims in the case. Id. at 258. The implications of Sony and Vault are explored in depth in Alfred P. Ewert & Irah H. Donner, Will the New Information Superhighway Create "Super" Problems For Software Engineers? Contributory Infringement of Patented or Copyrighted Software-Related Applications, 4 Alb. L.J. Sci. & Tech. 155 (1994).

[54] Id. at 257. Quaid may also have decompiled the Vault program to get access to information needed to "spoof" the Prolok software. Id. at 268. Even though this would have violated an express term of Vault's shrinkwrap license, the Fifth Circuit decided that this aspect of the shrinkwrap license was preempted by operation of copyright law. Id. at 269. The argument that decompilation is copyright infringement is discussed infra notes -- and accompanying text.

[55] Section 117(1) of the copyright statute enables owners of copies to make a copy of the program so long as the copy "is created as an essential step in the utilization of the computer program in

The contributory infringement claim arose from Quaid's development of software specially designed for use by consumers to enable them to bypass Vault's copy-protection system and to make illicit copies of programs protected by Vault's software.[57] The appellate court took its cue from the Supreme Court's *Sony* decision and focused its inquiry on whether Quaid's software was capable of substantial noninfringing uses. Quaid persuaded the Court of Appeals that copyright law gave people who bought commercial software off-the-shelf rights to make backup copies of their programs, as well as rights to copy in order to use and to engage in reverse analysis of the programs.[58] To the extent that the Louisiana shrinkwrap enforcement law was attempting to frustrate operation of federal policy, it should, Quaid argued, be preempted.[59] The appellate court agreed, deciding that Ramkey had a substantial noninfringing use as an aid to consumer exercise of backup copying rights under copyright law.

What killed the market for Vault's software and other similar products was not its defeat in this case, but marketplace competition that gave an edge to software developers willing to sell uncopy-protected versions of its products.[60] Notwithstanding the vulnerable nature of their products and the absence of commercially acceptable forms of technological protection for these products, the software industry as a whole has prospered.[61] This has not, of course, stopped software industry associations from vociferous complaints about "piracy" of their products, both domestically and abroad.[62]

C. *Sega v. Accolade*

---

conjunction with a machine and that it is used in no other manner." 17 U.S.C. §117(1). See Vault, 847 F.2d at 261.

[56] Id.

[57] Id. at 261-67. The most interesting (if least discussed) claim in the case was the second of Vault's two derivative work right claims. One claim focused on the appropriation of a code segment in an earlier version of Ramkey. The Court of Appeals found this code segment too small a part of the work to be of copyright concern. Id. at 267. Lurking in the case may have been another contributory infringement claim as to Vault's derivative work right. Quaid sold software that when used in conjunction with Vault's software adapted or recast it so that it didn't operate in its intended manner. This issue was more squarely presented in Lewis Galoob Toys, Inc. v. Nintendo of America, Inc., 780 F. Supp. 1283 (N.D. Cal. 1991), aff'd, 964 F.2d 965 (9th Cir. 1992) (game genie that altered play of Nintendo games held not to infringe derivative work right).

[58] See 17 U.S.C. §117, discussed in *Vault*, 847 F.2d at 263-66.

[59] The lawsuit was brought in the state of Louisiana because this state had adopted a law validating, as a matter of contract law, common terms of software shrinkwrap licenses. See Louisiana Software License Enforcement Act, La. Rev. Stat. §51:1961 et seq. (West 1987). For the court's discussion of this statute and its preemption analysis, see *Vault*, 847 F.2d at 268-70.

[60] See, e.g., Barlow, supra note --.

[61] Id.

[62] See, e.g., David Hornick, Combating Software Piracy: The Softlifting Problem, 7 HARV. J. L. & TECH. 377 (1994) (discussing the problem and strategies for coping with it).

A different kind of circumvention issue was presented in Sega Enterprises, Ltd. v. Accolade, Inc.[63] Sega argued that it had chosen to distribute its computer programs in machine-readable form in order to keep information, such as the technical specifications for its program-to-program or program-to-hardware interfaces embedded in the texts of its programs, as a trade secret. It alleged that decompilation or disassembly of its programs as a means of getting access to such trade secret information infringed its copyrights. Even if Accolade's videogames did not contain infringing code from the Sega programs, Sega thought that Accolade's games should nonetheless be enjoined from the market as "fruit of the poisonous tree" of decompilation.[64]

The Ninth Circuit Court of Appeals rejected Sega's argument, holding that decompilation of computer programs for a legitimate purpose, such as to get access to information necessary to construct a program that will interoperate with another program, constituted fair use, as a matter of law.[65] Although Accolade clearly had a commercial motive for decompiling Sega's programs, its principal purpose in making copies of Sega programs was in order to study and analyze the ideas in the program.[66] The court was unpersuaded that Sega's programs should be treated as unpublished works because they had been widely distributed in the marketplace.[67] The court recognized that a ruling in Sega's favor would be tantamount to giving Sega patent-like protection for the functional requirements needed to achieve compatibility,[68] and decided that this would be contrary to Congressional intent to protect only expression in programs, not ideas or other functional design elements.[69] Having used the information obtained through reverse analysis to develop its own original, noninfringing games, Accolade deserved the same chance to compete in the marketplace as other authors who had taken ideas but not expression from other works in preparing their own.[70]

---

[63] 977 F.2d 1510 (9th Cir. 1992). See also Atari Games Corp. v. Nintendo of America, Inc., 975 F.2d 832 (Fed. Cir. 1992). See generally Symposium on Copyright Protection and Reverse Engineering of Software, 19 U. DAYTON L. REV. 837 (1994).

[64] See Sega Ent., Ltd. v. Accolade, Inc., 785 F. Supp. 1392 (N.D. Cal.), rev'd, 977 F.2d 1510 (9th Cir. 1992). See also Jessica Litman, Copyright and Information Policy, 55 LAW & CONTEMP. PROBS 185 (1994) (discussing the decompilation debate).

[65] Sega, 977 F.2d at 1514. See generally Julie E. Cohen, Reverse Engineering and The Rise of Electronic Vigilantism: Intellectual Property Implications of "Lock-Out" Programs, 68 S. CAL. L. REV. 1091 (1995).

[66] Sega, 977 F.2d at 1522-23. See Leo J. Raskind, Reverse Engineering, Unfair Competition, and Fair Use, 70 MINN. L. REV. 385 (1985) (predicting that the copying-to-engage-in-reverse-analysis provision of the Semi

[67] Sega, 977 F.2d at 1524-26. The Court of Appeals cited to its prior decision in Galoob as having resolved this issue. Id. at 1526, n. 9, citing Galoob, 964 F.2d at 971.

[68] Sega, 977 F.2d at 1526-27.

[69] Id.

[70] Sega, 977 F.2d at 1523.

D. Reflections on *Sony, Vault, and Sega*

Among the reasons these cases are of interest is the importance they place on copyright as a law that must strike a balance among competing interests.[71] Copyright does not just protect the interests of copyright owners; it also protects the interests of users. These cases reflect a tradition that views copyright as a limited grant to authors for the purpose of achieving a larger societal goal, one embedded in the U.S. Constitution, of promoting knowledge and public access to it.[72] When new technologies have raised questions that are not easily answered by existing law, courts have tended to construe the law in light of these larger societal purposes.[73] These larger purposes of copyright law and the notion of copyright as a law that strikes balances are given short shrift in the White Paper. This is especially evident in the White Paper's discussion of its proposed anti-circumvention provision.

III. PROBLEMS WITH THE WHITE PAPER'S PROPOSED ANTI-CIRCUMVENTION PROVISION

The Clinton Administration's White Paper contains a far more extensive discussion of the various kinds of technological protection that copyright owners may find useful for protection of digital versions of their works in networked environments than of the policy analysis underlying its broad anti-circumvention provision.[74] Apart from indicating that technological protection for copyrighted works may be ineffective unless the law "provides some protection for the technological processes and systems used to prevent or restrict unauthorized uses of copyrighted works,"[75] the White Paper says only that

> [t]he Working Group finds that prohibition of devices, products, components, and services that defeat technological methods of preventing unauthorized use is in the public interest and furthers the Constitutional purpose of copyright laws. Consumers of copyrighted works pay for the acts of infringers; copyright owners have suggested that the price of legitimate copies of copyrighted works may be higher due to infringement losses suffered by copyright owners. The public will also have access to more copyrighted works if they are not vulnerable to the defeat of copy protection systems.[76]

---

[71] See, e.g., Sony, 464 U.S. at 429.

[72] Id.

[73] See, e.g., Sega, 977 F.2d at 1526-27.

[74] White Paper, supra note --, at 177-99 (discussing technological protection), 230-33 (discussing the proposed anti-circumvention provision, little of which is policy analysis).

[75] White Paper, supra note --, at 230.

[76] Id.

It consequently recommends adoption of a rule that would make it illegal for persons (1) to import, manufacture or distribute (2) any device, product, or component incorporated into a device or product, or to offer or perform a service, (3) the primary purpose or effect of which (4) is to avoid, bypass, remove, deactivate, or otherwise circumvent, (5) without authority of the copyright owner or the law, (6) any process, treatment, mechanism, or system which prevents or inhibits the exercise of any of the exclusive rights under Section 106.[77] Remedies would include injunctive relief, impoundment, actual or statutory damages and, in the case of repeated violations, up to treble damages, as well as recovery of costs and attorney fees.[78]

The White Paper does not inform readers that adoption of its anti-circumvention proposal would effectively overrule the Supreme Court's contributory infringement ruling in the *Sony* case.[79] Nor does it discuss the implications of its anti-circumvention provision for the appellate court rulings in the *Vault* and *Sega* cases. As shown below, it is plausible to construe the White Paper as aiming to overturn, sub silencio, both of these rulings as well.

The White Paper asserts that several "precedents" support adoption of its proposed anti-circumvention provision.[80] The other laws it cites are, however, much more narrowly tailored than the anti-circumvention provision the White Paper recommends.[81] The White Paper also understates the impact its anti-circumvention provision will have for the public domain and for undermining other free expression values. In its discussion of the anti-circumvention provision, as in so many other parts of the document,[82] the White Paper is best understood as a skillful advocacy document rather than as a balanced public policy framework for adapting copyright law to digital networked environments.

A. Appellate Decisions Implicitly Jeopardized By the Anti-Circumvention Provision

The White Paper is silent about the implications of its anti-circumvention provision for the continued viability of such decisions as *Sony*, *Vault*, and *Sega*. In its

---

[77] Id., Appendix at 4.

[78] Id., Appendix at 5-6. The preliminary draft report of the Intellectual Property Working Group (known as the "Green Paper" proposed that violation of the anti-circumvision provision be a felony. See Green Paper, supra note --, at 129.

[79] Green Paper, supra note --, at 126.

[80] White Paper, supra note --, at 233.

[81] See infra notes -- and accompanying text.

[82] See, e.g., James Boyle, The Information Toll Road, WASH. TIMES, Dec. xx, 1995; Peter A. Jaszi, Caught in the Net of Copyright, -- ORE. L. REV. -- (forthcoming 1996); Jessica Litman, The Exclusive Right to Read, 13 CARDOZO ARTS & ENT. L.J. 29 (1994) (critical of Working Group's browsing-as-infringement analysis); Pamela Samuelson, The Copyright Grab, WIRED 4.01, p. 134 (Jan. 1996). But see Jane C. Ginsburg, Putting Cars on the "Information Superhighway": Authors, Exploiters, and Copyright in Cyberspace, 95 COLUM. L. REV. 1466 (1995).

predecessor document, known as Green Paper on Intellectual Property and the NII, the Intellectual Property Working Group had made clear that it intended for an identically worded anti-circumvention provision to overturn the contributory infringement standard set forth in Supreme Court's *Sony* decision.[83] The Green Paper offered this complaint about the Court's standard: "Under the *Sony* decision, a manufacturer is not liable for contributory infringement if the device is *capable* of a 'substantial noninfringing use,' even if the device is *rarely* or *never* put to those uses, and even if the use to which it is *primarily* put is infringing."[84]

The Green Paper was also explicit about who would have standing to challenge anti-circumvention technologies. This is an issue that goes unmentioned in the White Paper. Under the Green Paper's interpretation of its anti-circumvention provision, any copyright owner whose work *could be* infringed by a particular circumvention technology would have standing to sue the maker of it for circumvention-infringement,[85] regardless of whether *any* infringing copies had *ever* been made through use of that circumvention technology (let alone *any* infringing copies made of *that* copyright owner's works).[86] The only parties explicitly disabled from bringing suit under the Green Paper's approach would have been firms whose technologies could be circumvented by that particular device or technique.[87]

Vault is mentioned only once in the White Paper wherein it is characterized as a "controversial decision."[88] The White Paper gives no explanation about the nature of the controversy, nor any citation to a source describing the case as controversial. In analyzing the facts of*Vault* under the White Paper's proposed anti-circumvention provision, Quaid's liability would seem to turn on whether a court decided that the primary *effect* of Ramkey was to aid the making of illicit copies of software. On this issue, each party would likely offer expert testimony about its likely primary use, data on actual use likely being unavailable.[89] It is not difficult to imagine that a judge,

---

[83] Green Paper, supra note --, at 126

[84] Id. (emphasis in original).

[85] The Green Paper would have made violation of the anti-circumvention provision a special new form of copyright infringement. See infra note --.

[86] See Green Paper, supra note --, at 128-30.

[87] Id. at 130.

[88] White Paper, supra note --, at 56, n.169.

[89] In cases involving the Electronic Communications Privacy Act which forbids manufacture or distribution of devices that are "primarily useful" for illicit wiretapping, courts have generally relied on expert testimony, usually from law enforcement officials, concerning the likelihood of use for illicit purposes. See, e.g., U.S. v. Pritchard, 773 F.2d 873, 875-78 (7th Cir. 1985) (testimony of FBI agent sufficed to find device primarily useful for surreptitious listening) and U.S. v. Wynn, 633 F. Supp. 595 (C.D. Ill. 1986) (testimony of two officers constituted sufficent evidence that primary use would be illicit wiretapping). Because the issue of whether the primary purpose or effect of a technology would be to bypass or circumvent technical protection would, under the White Paper's anti-circumvention provision, be an issue of fact, summary judgment may rarely be granted. Pritchard, 773 F.2d at 878. Although the White Paper recommends enactment of remedy provisions that would give courts

faced with conflicting speculative expert evidence of this sort, would ultimately conclude that it is implausible to believe that the primary use of Quaid's software would be to help consumers make legitimate backup copies. If there is reason to think that the IP Working Group would support a ruling in Quaid's favor in the litigation with Vault, it is because the Green Paper took the position that the only persons who should be able to bring suit against the manufacturer of a circumvention technology are those copyright owners whose works could be infringed by the circumvention technology, rather than manufacturers of technologies that could be circumvented, such as Vault.[90]

Given *Sega* 's prominence as a digital copyright precedent,[91] it might seem surprising that neither the Green Paper nor the White Paper makes any mention of that decision.[92] This omission becomes more understandable--as well as more ominous--if one knows that the officials in the Clinton Administration have publicly questioned the *Sega* decision, both domestically and abroad.[93] Armed with knowledge of official distaste for this decision, one can discern the anti-*Sega* agenda it may contain.

Recall that Sega had argued that it made a conscious decision to distribute its videogames in machine-readable form only because it did not want the public to have access to human-readable forms of its programs. This arguably makes object code distribution a "process, treatment, mechanism, or system" for protecting the human-readable text of the program from unauthorized disclosure or use. The primary purpose or effect of decompilation would be to interfere with this objective Sega had in choosing to distribute object code to the public. Although decompilation may also a "service" falling within the strictures of the anti-circumvention provision, one must consider the potential application of a built-in limitation on the scope of the anti-circumvention provision. It recognizes that not only the copyright owner, but also the law of copyright, can authorize derogations from the exclusive rights granted to copyright owners.[94] It might then seem that under the Ninth Circuit's*Sega* decision, decompilation for legitimate purposes, such as gaining access to program interfaces, would fall within this limitation. Two factors may undercut this argument: first, the

---

discretion to reduce or remit damages if a manufacturer has innocently violated the anti-circumvention provision, White Paper, supra note --, Appendix at 6,

[90] Green Paper, supra note --, at 130. Quaid should just feel lucky its principals won't have to go to prison for having developed Ramkey because the White Paper dropped the felony penalty for violation of the anti-circumvention rule.

[91] See, e.g., Cohen, supra note --.

[92] Neither document mentions the appellate court rulings that have held that functional requirements for achieving compatibility with other programs are beyond the scope of copyright in computer programs. See, e.g., Computer Associates Int'l, Inc. v. Altai, Inc., 982 F.2d 693 (2d Cir. 1992).

[93] See, e.g., Rob Rossi, A Brash, New Voice for the IP Arena: Patent & Trademark Commissioner Bruce Lehman Stirs Up Controversy Among Silicon Valley Practitioners, The Recorder, p. 1, Feb. 17, 1994.

[94] White Paper, supra note --, Appendix at 4 ("without authority of the copyright owner *or the law*") (emphasis added).

White Paper endorses proposed changes to commercial law that would validate, as a matter of contract law, mass market license terms that forbid decompilation or disassembly of computer program code;[95] and second, the White Paper asserts that copyright owners are free to make use of any "process, treatment, mechanism, or system" to deny consumers the opportunity to make unauthorized uses of their works without regard to fair use.[96] If by distributing their works in other than human-readable form, copyright owners wish to deny consumers an opportunity to get access to information in the work, the White Paper would seem to defer to that decision.

The failure to discuss the possible implications of the anti-circumvention provision for Sega and kindred precedents is ominous because several commentators on the Green Paper raised concerns about the potential application of this provision to decompilation.[97] If the White Paper did not mean to cast doubt on the legality of decompilation following enactment of the anti-circumvention provision, it would probably have said so. In the absence of this clarification, software developers who do engage in decompilation have reason to be concerned about the implications of the anti-circumvention provision recommended in the White Paper for their routine decompilation activities.

B. Why the "Precedents" Cited Do Not Support the White Paper's Proposed Anti-Circumvention Rule

To show that its anti-circumvention rule is not unprecedented, the White Paper mentions several other laws : (1) a provision from a law regulating digital audio tape (DAT) recorders; (2) a provision from the Communications Act of 1934 that regulates devices that can be used to decrypt satellite transmissions of television programs; (3) a NAFTA treaty provision about decryption of satellite transmissions; and (4) a law enacted in the United Kingdom regulating circumvention of copy-protection systems.[98] Each of these laws is, however, a considerably narrower "precedent" than the White Paper reveals.

The DAT anti-circumvention and satellite signal decryption provisions are less close analogues to the anti-circumvention provision proposed in the White Paper for several reasons. For one thing, the DAT and satellite decryption laws each aimed to protect one very specific, well-defined technology, unlike the White Paper provision

---

[95] Id. at 49-59. If shrinkwrap license terms were enforceable as a matter of contract law, that would arguably undercut the decompilation-as-fair-use argument because courts have been reluctant to find fair use when a use has been licensed on restrictive terms. See, e.g., Advanced Computer Services v. MAI Sys. Corp., 845 F. Supp. 356 (E.D. Va. 1994). See Mark A. Lemley, Intellectual Property and Shrinkwrap Licenses, 68 S. CAL. L. REV. 1239 (1995) (critical of proposed rules regarding enforceability of mass market licenses on decompilation of computer programs).

[96] White Paper, supra note --, at 231.

[97] See, e.g., Statement of the American Committee on Interoperable Systems in Response to Green Paper on Intellectual Property and the NII (1994). See also Samuelson, supra note --.

[98] White Paper, supra note --, at 233.

which may apply to hundreds, if not thousands, of unspecified technologies. Second, notwithstanding the "primary purpose or effect" language in the DAT provision[99] and the "primarily useful" language in satellite provision,[100] the specific technology being protected by each law was not one likely to be casually or unintentionally circumvented, but would rather have been specially designed for that purpose. Also, there was likely to be no market for the outlawed circumvention technologies that those laws addressed except as a means to defeat the targeted technology.[101] This suggests that even under the Supreme Court's standard in Sony, one could have regulated them. Third, both provisions responded to very specific, demonstrable problems, rather than to a range of possible unspecified problems, as the White Paper proposal would do.

An even more significant factor that makes the DAT law a narrower precedent than the White Paper admits is that a critical part of the legislative compromise embodied in the DAT law was an agreement that serial copy management systems (SCMS) would enable consumers to make usable first-generation private noncommercial copies.[102] SCMS inhibits only the making of perfect copies that could become "digital masters" from which multiple additional perfect copies might be made.

A factor that makes both the satellite provision and the U.K. law significantly narrower "precedents" than the White Paper acknowldges is that both have knowledge/intent requirements not found in the White Paper's proposed anti-circumvention provision.[103] The satellite provision, for example, requires not only that the device be primarily useful for an illicit purpose, but that its maker have *actual knowledge or reason to know* that the device is primarily of assistance in the unauthorized decryption of satellite programming.[104] The U.K. law permits a suit only "against a person who, *knowing or having reason to believe* that it will be used to make infringing copies...makes...any device or means *specifically designed or adapted* to circumvent the form of copy-protection employed...or publishes information intended to enable or assist persons to circumvent that protection."[105] Liability for making a device that can be used to circumvent a copy-protection system under this law is thus limited to situations where there is proof both of the developer's knowledge

---

[99] 17 U.S.C. §1002(c).

[100] 47 U.S.C. §605(e)(4).

[101] See, e.g.,

[102] See, e.g., Christine C. Carlisle, The Audio Home Recording Act of 1992, 1 J. INTELL. PROP. L. 335 (1994) and Michael Plumleigh, Comment, Digital Audio Tape: New Fuel Stokes the Smoldering Home Taping Fire, 37 UCLA L. REV. 733 (1990).

[103] See also Electronic Communications Privacy Act, 18 U.S.C. §2512(1)(b) (prohibiting intetional manufacture or possession of any electronic device "knowing or having reason to know that the design of such a device renders it primarily useful for the purpose of...surreptitious interception" of wire transfers).

[104] 47 U.S.C. §605(e)(4).

[105] Copyright, Designs & Patent Act of 1988 §296 (emphasis added).

of the likelihood that consumers will use it for infringing purposes and a specific intent to enable circumvention during the design phase of its development. Thus, these laws do not support the broad anti-circumvention provision recommended in the White Paper.

The White Paper also does not mention other more narrowly drawn laws that regulate "dual use" technologies, that is, technologies having some uses that are lawful, and some that may be illicit. One such law is the cable signal descrambling provision of the Communications Act of 1934, which prohibits the theft of cable service by "the manufacture or distribution of equipment *intended* by the manufacturer or distributor...for unauthorized reception of any communications service."[106] Even though theft of cable services was an industry problem, Congress decided not to subject manufacturers, distributors and retailers to liability "if they are engaged in the production and sale of a device or equipment...merely because the same device or equipment is capable of being used for unauthorized reception of cable service, if they do not provide the equipment with the intent or specific knowledge that it will be used for the unauthorized reception of cable service."[107]

Nor does the White Paper give consideration to the reasons Congress adopted the "substantial noninfringing use" standard in the patent law which the Supreme Court carried over to copyright in its Sony decision. Patent law does not shield manufacturers of dual use technologies from liability out of a desire to molly-coddle would-be infringers, but because the public has a legitimate interest in having access to technologies that can be put to noninfringing uses. As the Supreme Court observed in its *Sony* decision, a balance must be struck "between [the rightsholder's] legitimate demand for effective--not merely symbolic--protection of the statutory monopoly, and the rights of others freely to engage in substantially unrelated areas of commerce."[108] The White Paper makes no effort to engage in such balancing.

C. Impact of the White Paper's Anti-Circumvention Provision on the Public Domain and Fair Use

Unlike the White Paper, the Green Paper acknowledged the legitimacy of "some concerns regarding [the anti-circumvention] proposal, particularly with regard to works whose term of copyright protection expires but are still protected by anti-copying systems, and works in the public domain."[109] On this issue, the White Paper offers only legalistic arguments about why there is no cause for concern.

It argues, for example, that those who manufacture and distribute of devices whose primary purpose and effect is to defeat technological protection for works in the

---

[106] 47 U.S.C. §533(a)(2) (emphasis added).

[107] H.R. Rep. 98-934 at 157, reprinted in 1984 U.S.C.C.A.N. 4655.

[108] Sony, 464 U.S. at 442.

[109] Id. at 130.

public domain would not be governed by its anticircumvention provision.[110] Second, it argues that "a protection system on copies of works in the public domain would not qualify with respect to such copies as a system which 'prevents or inhibits the violation of any of the exclusive rights of the copyright owner under Section 106.'"[111] The problem with these arguments is that they would only hold true if firms used different kinds of technological protection for public domain materials than they and others in the information industry used for works protected by copyright. As long as the same encryption algorithm is used to protect both kinds of works, chances are that a court would regard the algorithm as a "process, treatment, mechanism, or system" to prevent or inhibit violations of copyright's exclusive rights provisions. There is no reason to assume that firms will be foolish enough to use anything other than copyright industry standard encryption techniques when distributing public domain materials.

In addition, the White Paper asserts that even if technological protection were applied to copies of works in the public domain, that protection would attach "only to those particular copies--not to the underlying work itself."[112] One who wished to freely copy public domain materials could always do so from a source unencumbered by technological protection. The White Paper also indicates that technological protection "that restricts the ability to reproduce the work by technical means does not prevent reproduction by other means (such as quoting, manually copying, etc.)."[113] The first of these two arguments holds true only if there is in existence a copy of the work that is unhampered by technological protection and access to it is feasible without undue expense or difficulty. The White Paper's approach would implicitly seem to incent firms to acquire the extant unencumbered public domain copies in order block public access to them, for then only technologically protected copies would be available, and these could not be tampered with. It is also unclear why the public should have to go to some remote source to get unencumbered access to a public domain work if they already have an electronic copy of it, and its technological protection can be bypassed without the bypasser doing so to infringe a copyright.

The White Paper does not directly make the suggestion, but a careful reader of its discussion of the anti-circumvention provision may find herself wondering if the public domain is a viable concept in the electronic environment. Is it perhaps an artifact of the print era that will die out in the next era? Historically, an important role of the public domain has been to enable competitive publication of works after its author and first publisher had had a chance to recoup their investments and make sufficient profits to justify further investments in producing and distributing creative

---

[110] White Paper, supra note --, at 232.

[111] Id., quoting from its proposed anti-circumvention provision.

[112] Id.

[113] Id., n.567.

works.[114] In the print world, it has been commercially feasible for competing publishers to print and distribute copies of works whose copyright terms had expired. Because each printer who wanted to sell copies of a particular public domain work would have to incur the same substantial costs if they wanted to publish the work, it was not possible to take a free ride on the previous publisher's investments.

A firm wanting to produce electronic versions of, for example, Jane Austen's novels faces a different situation. Anyone who acquires an electronic copy of this firm's product will have the means to become an alternative publisher of the same works.[115] Unless the firm adds a substantial amount of new material to enable it to claim a derivative work copyright or unless it uses technological means to protect its electronic copies, it won't have a chance of recouping its investment in making the Austen novels available electronically. The first purchaser would, under standard application of copyright theory, be entitled to download the electronic file and either distribute it for free or in competition with the firm that produced it.

Some have argued that copyright protection should be available for digitized versions of public domain materials.[116] It is, however, difficult to accept that digitization satisfies the minimum creativity standard that the Supreme Court has said is required in order for copyright protection to be available to a work.[117] A short term of anti-cloning protection for digitized versions of public domain works would be another alternative,[118] but as yet, policymakers have been resistant to addressing legal protection issues under alternative regimes.

As regards works developed and distributed in electronic form, there is some reason to doubt whether they will ever enter the public domain. By the time works first published in electronic form reach copyright expiration dates, it is far from clear that the media and equipment now used to read those electronic copies will still be available.[119] In addition, owners of copyrights in works published in electronic form

---

[114] See, e.g., Wendy J. Gordon, Inquiry on the Merits of Copyright: The Challenges of Consistency, Consent, and Encouragement Theory, 41 STAN. L. REV. 1343 (1989); Jessica Litman, The Public Domain, 39 EMORY L.J. 965 (1990).

[115] This issue has recently been presented in ProCD, Inc. v. Zeidenberg, 1996 U.S. Dist. LEXIS 167 (W.D. Wis. 1996) (competitive copying of public domain material from another firm's electronic product held not illegal).

[116] See, e.g., Dennis S. Karjala, Copyright and Misappropriation, 17 U. DAYTON L. REV. 885 (1992).

[117] Feist, 499 U.S. at 352-57.

[118] See, e.g., J.H. Reichman, Legal Hybrids Between the Patent and Copyright Paradigms, 94 COLUM. L. REV. 2432 (1994); Pamela Samuelson, et al., A Manifesto Concerning the Legal Protection of Computer Programs, 94 COLUM. L. REV. 2308 (1994).

[119] See, e.g., Peter S. Graham, Intellectual Preservation and Electronic Intellectual Property, IMA Proceedings, supra note --, at 153-68.

may well decide to program copies to self-destruct prior to the date of expiration.[120] Following the expiration date, holders of these now-expired rights might choose to make the works available only by online access under restrictive contract terms, such as those West Publishing now employs with public domain statutes and judicial decisions.[121]

Many copyright owners will not wait until shortly before copyright expiration dates to program electronic copies to self-destruct or become inoperative after a particular date or after a certain number of uses. Self-destruct features are likely to be useful as a way of technologically enforcing short term usage licenses that may represent the future of commerce in digital works on the NII. The White Paper contemplates short-term licenses for digital copies of copyrighted works,[122] but does not discuss self-destruct features or otherwise explore the consequences of these licenses for the public domain. Terms of usage licenses are likely to be among the items of information designated as copyright management information, any tampering with which would be both a felony and a civil wrong under the White Paper's legislative proposals.[123]

The White Paper seems to accept as a natural development that in the future the public will have access to works--whether they are protected by copyright or not--on whatever terms and conditions copyright owners choose to make them available.[124] In its view, the law of copyright imposes no responsibilities on rightsholders. Should rightsholders choose to make works available in a form making it impossible to make fair uses of them, for example, the White Paper sees no reason to be concerned about this development, for the fair use doctrine

> does not require a copyright owner to allow or to facilitate unauthorized access or use of a work. Otherwise, copyright owners could not withhold works from publication; movie theatres could not charge admission or prevent audio or video recording; museums could not require entry fees or prohibit the taking of photographs. Indeed, if the provision of access and the ability to make fair use of copyrighted works were required of copyright owners--or an affirmative right of the

---

[120] Tampering with a self-destruct feature might well be a felony if the feature is included in the copyright management information protected under proposed 17 U.S.C. §1202. See White Paper, Appendix at 4.

[121] Every transaction with Westlaw produces this notice: "No part of a WESTLAW transmission may be copied, downloaded, stored in a retrieval system, further transmitted or otherwise reproduced, stored, disseminated, transferred or used, in any form or by any means except as permitted in the Westlaw Subscriber agreement or with West's prior written agreement."

[122] White Paper, supra note --, at 49-59.

[123] White Paper, supra note --, at 235, Appendix at 4-7.

[124] See also Jane C. Ginsburg, Copyright Without Walls, 42 REPRESENTATIONS 53 (1993) (discussing uses of contracts to avoid fair use and other public policy limitations on exclusive rights embodied in copyright law).

public--even passwords for access to computer databases would be considered illegal.[125]

In view of the fact that the White Paper treats every electronic access to or use of a copy of a copyrighted work as a prima facie infringement,[126] and regards the first sale doctrine as inapplicable in the electronic environment[127] and fair use as unavailable if a use can be licensed,[128] the power of rightsholders in the electronic environment would seem to be truly awesome. Technological protection, along with the freedom from circumvention technologies that the White Paper proposal would bring about, is an important component of a larger maximalist strategy for shifting power away from consumers and toward publishers.

There is, however, an alternative perspective on copyright law, one that conceives of fair use as a "right" of users[129] and that conceives of public access to public domain works and unprotectable elements embodied in copyrighted works as a critical part of the quid pro quo that has long been part of copyright tradition.[130] These policies which are ignored in the White Paper suggest that there is a need for further discussion and debate to take into account the continuing public interest in access to information before charting a future in which all content may be technologically protected and any circumvention of that protection is declared illegal.

D. Other Potential Effects of the Anti-Circumvention Provision

The White Paper's discussion of intellectual property and the NII presupposes that copyright is, by far, the most important form of intellectual property right affected by the NII. This importance is conveyed in part by the proportion of the White Paper that discusses copyright law, as compared to other intellectual property laws.[131] Implicit in the White Paper's discussion of copyright is a conception of this law that is

---

[125] White Paper, supra note --, at 231. No discussion of the White Paper's views on fair use and public access to information would be complete without mentioning its classic response to concerns that its policies will disadvantage further the "information have-nots" in society: "Some participants have suggested that the United States is being divided into a nation of information 'haves' and 'have nots' and that this could be ameliorated by ensuring that the fair use defense is broadly generous in the NII context. The Working Group rejects the notion that copyright owners should be taxed--apart from all others--to facilitate the legitimate goal of 'universal access.'" Id. at 84.

[126] Id. at 64-66.

[127] Id. at 90-95.

[128] Id. at 73-84.

[129] See, e.g., Princeton University v. Michigan Document Services, 1996 U.S. App. LEXIS 1919 (6th Cir. 1996) and Bateman v. Mnemonics, Inc., 37 U.S.P.Q.22d (BNA) 1225 (11th Cir. 1995).

[130] See, e.g., Sega, 977 F.2d 1510; Paul J. Heald, Payment Demands for Spurious Copyrights: Four Causes of Action, 1 J. INTELL. PROP. L. 259 (1994).

[131] One hundred twenty-five pages of the White Paper are devoted to a discussion of copyright law, as compared with twenty on patent law, five on trademark law, and two on trade secret law.

widely shared by the public: that it is a law that concerns itself with protecting movies, books, sound recordings, and other commercially distributed works.[132]

Very little attention is given to trade secrecy law in the White Paper.[133] The White Paper makes no mention of what kind of relationship, if any, it contemplates between copyright and trade secrecy law in the NII. In the past these two laws have regulated very different kinds of works in very different ways: Trade secrecy law has protected documents valued for the secrets they contain against the use of improper means to obtain the secrets and against disclosures in breach of confidential relationships or contracts, whereas federal copyright law has protected documents against unauthorized copying following their first publication.[134] Although authors had some common law protection against unauthorized publications of their manuscripts,[135] it was not until1978 that federal copyright took on the task of protecting every original work of authorship from the moment of its first fixation in a tangible medium.[136] This protection lasts for life of the author plus fifty years,[137] or if the work's author is a corporation and the work is unpublished, the copyright lasts for one hundred years.[138]

Because copyright law now spreads its protective mantle over unpublished works as well as published ones, new opportunities exist for firms to use both copyright and trade secrecy law, or whichever of the two would best serve its interests in a particular case.[139] As a consequence, it may now behoove possessors of electronic documents containing information their possessors want to keep secret to reconceive their legal protection strategies away from reliance on trade secrecy alone. If they conceive of their works in copyright terms, they may be able to have the benefit

---

[132] See, e.g., Jessica Litman, Copyright As Myth, 53 U. PITT. L. REV. 235 (1991) (discussing popular conceptions of copyright).

[133] White Paper, supra note --, at 173-75. One is told, for example, that trade secrecy, unlike copyright and patent, is a state rather than a federal law, and some complex questions may arise about which state's trade secrecy law is violated. Id.

[134] For a general discussion of the relationship between trade secrecy and copyright law in the context of computer software, see, e.g., David Bender, Protection of Computer Programs: The Copyright/Trade Secret Interface, 47 U. PITT. L. REV. 907 (1986).

[135] See, e.g., Ralph S. Brown, Unification: A Cheerful Requiem for Common Law Copyright, 24 UCLA L. REV. 1070 (1977)

[136] 17 U.S.C. §§102(a), 302(a). For a discussion of changes wrought by the Copyright Act of 1976 as regards federal protection for unpublished works, see, e.g., Brown, supra note --.

[137] 17 U.S.C. §302(a).

[138] 17 U.S.C. §302(c).

[139] For a discussion of copyright policies favoring public access to information when a work is commercialized, see Robert A. Kreiss, Accessability and Commercialization in Copyright Theory, 43 UCLA L. REV. 1 (1995). See also Pamela Samuelson, CONTU Revisited: The Case Against Copyright Protection for Computer Programs in Machine-Readable Form, 1984 DUKE L.J. 663 (1984) (pointing out that, unlike patent law, copyright has previously not had to require disclosure of contents of works because publication of the works brought about disclosure).

of both laws, not just one.[140] Technological means to protect digital secrets will also be an attractive strategy, whether a firm conceives of its content in copyright or trade secret terms.

When considering how to distribute their content via the NII, possessors of trade secrets would be well-advised to use an encryption algorithm or other technology commonly used by the copyright industries. If they do this and conceive of their content as protected by copyright law as well as trade secrecy law, then any technology that might be used to circumvent or bypass the technological protection they are using to protect their secrets could be attacked under the White Paper's anti-circumvention provision. The trade secret owner would seem to have standing to sue to challenge the circumvention technology under the White Paper's standard.

Conceiving of electronic trade secret documents as unpublished copyrighted works would also broaden the class of documents pertinent to a determination about the primary purpose or effect of a particular circumvention technology. If a technique is useful to decrypt unpublished copyrighted works containing trade secrets as well as to decrypt encrypted sound recordings or movies, that increases the chances the technology can be outlawed under the White Paper's anti-circumvention provision.

Also potentially pertinent would be the utility of a particular decryption technology to undo technological protection for ordinary private electronic communication between individuals. This content too, after all, is protectable by copyright law from the moment the communication was first fixed in digital form.[141] Once one broadens the realm of technologically protected content that will count in measuring primary purpose and effect of a circumvention technology in this way, there may be almost no circumvention technology that could avoid application of the White Paper's anti-circumvention provision.

The purpose of this discussion is to show that in some very subtle but important ways, copyight policy and security policy are on a path of convergence. Copyright law is being readied to take on a new set of functions as a law that will protect the security of electronic information. The White Paper's anti-circumvention provision would permit copyright law to be invoked to enforce the interests of those who seek to protect the contents of their works *as secrets* by whatever technological process or system they choose.[142] It is a brave new world for copyright--as well as an inversion

---

[140] For that matter, copyright owners may have want to reconceive their works in trade secret terms as well. By disseminating their content only in encrypted form to individual licensees who might be bound by contract terms not to disclose their contents, copyright owners might be able to market their works widely and claim them as unpublished works containing trade secrets as well. This would not concern drafters of the White Paper, see supra note -- and accompanying text, but traditional copyright doctrine would have concerns about this, see e.g., Kreiss, supra note --.

[141] 17 U.S.C. §§102(a), 302(a).

[142] In trying to understand the transformation of copyright that the anti-circumvention provision may bring about, it is worth noting that the Green Paper proposed to include the anti-circumvention

of what has been considered its constitutional purpose[143]--to be transformed into a law whose principal function is to ensure that people cannot get access to publicly disseminated information, including that which is in the public domain.

If the White Paper's broad anti-circumvention provision is enacted, copyright law may not only become a general misappropriation law to protect digital trade secrets, private communications, as well as movies and sound recordings. It can also become an anti-computer hacker law. Consider, for example, the famous case of Robert Morris and his "Internet worm" under the terms of the White Paper's anti-circumvention provision.[144] Many computer systems employ password software as a process to prevent unauthorized access to and use of electronic information stored on the computers. This would make password systems a class of protected technology under the anti-circumvention proposal. A primary effect, if not a primary purpose, of Morris' program was to defeat the Unix password system used on approximately 6000 computers nationwide. Morris's software probably is probably a "device" under the anti-circumvention provision and he would be a "manufacturer or distributor" of this device. So he could probably be sued under the anti-circumvention provision. Perhaps wiretapping and other forms of electronic espionage could be attacked under teh anti-circumvention provision as well.

Consider also whether state or local law enforcement officials might run afoul of the anti-circumvention provision if they developed software or some other technique or device to get unauthorized access to the encrypted files of a mobster. As long as the mobster used an encryption algorithm widely used by copyright industries, the police might violate the law because the primary purpose or effect of the technique they were using might undermine the sanctity of this form of technological protection. It is important to realize that the White Paper's anti-circumvention provision does not contemplate that someone can escape liability by showing that his or her particular use was legitimate. The question is whether the primary purpose or effect of the circumvention technology is to enable unauthorized access and copying of works whose owners have chosen to protect by technological means. The mobster would surely have chosen this particular form of technological protection in order to prevent others (including the police) from having unauthorized access to and from being able to make unauthorized copies of his files. There will probably be enough originality in

---

provision as section 512 of the copyright statute and to make violation of the anti-circumvention provision as a new kind of copyright infringement. Green Paper, supra note --, at 128. The Green Paper would also have made violation of the anti-circumvention provision a felony as well as a civil wrong. Id. at 129. After encountering some resistance at international meetings to the proposal to integrate the anti-circumvention provision into the heart of copyright law and from electronic equipment manufacturers about the felony provision, the Green Paper approach was dropped. Even though the anti-circumvention provision would now stand outside of the copyright law, its essential function is not substantially different from the original proposal.

[143] See supra note --.

[144] See U.S. v. Morris, 928 F.2d 504 (2d Cir. 1991). See generally Ted Eisenberg, et al., The Cornell Commission: On Morris and the Worm, in COMPUTERS UNDER ATTACK 253 (Peter J. Denning, ed. 1990).

the selection and arrangement of information in the files to qualify for copyright protection. Even in advance of any actual use of the technique against him or his confederates, the mobster would have standing to sue to enjoin use of the technique.[145]

Consider also whether a computer scientist would violate the anti-circumvention provision if he or she published a paper describing how to undo a particular encryption technique that was used by some copyright owners, and whether the publisher of this article would be liable as well.[146] If word about the decryption technique got out, as, of course, it would if the article was published, the primary effect of publication of the article might well be to bypass a means of technological protection for copyrighted works. The first amendment implications of this deserve serious attention before the White Paper's anti-circumvention provision is enacted.

The point of this discussion is not that it would be awful to have another form of legal protection against trade secret misappropriation or computer hacking, but that copyright law has historically not regulated these sorts of activities and it may not be well-suited to taking on the larger enforcement responsibilities for which content owners might want to employ it. Nor is the point of this discussion that mobsters will succeed in using the anti-circumvention provision to thwart legitimate law enforcement activities or that copyright industries will immediately start suing computer scientists and their publishers. Rather, the point is that sometimes there may sometimes be legitimate reasons to undo technological protection for documents or to allow information about circumvention techniques to be disseminated. The better approach may be to narrow the set of activities that could be regulated by an anti-circumvention provision, whether by adding knowledge or intent requirements, by limiting liability to technologies that were specially designed to harm copyright industries, and/or by focusing on the legitimacy or illegitimacy of particular actual uses of a technology rather than on uses to which the technology might be put. As Robert Frost once said:

Before I build a wall I'd ask to know

---

[145] If the mobster example seems too speculative or unsympathetic, consider the possibility of using the anti-circumvention provision to attack the National Security Agency's routine practice of intercepting electronic communications and attempting to discern the contents of these communications. They have surely developed some sophisticated techniques specially designed to undo the technological protection that the senders of the information employed to prevent unauthorized persons from getting access to and making copies or other uses of that information. Since anyone whose communications could be intercepted would have standing to sue the NSA for unauthorized development and use of techniques and software that could be used to undo technological protection they have employed, no standing problems would exist, as long as the person bringing the suit was willing to claim copyright in his or her encrypted communications.

[146] Offering or providing a service, the primary purpose or effect of which is to bypass or avoid technological protection or the like also runs afoul of the anti-circumvention provision. See also supra note -- and accompanying text concerning a U.K. statute that makes explicit that providing information that will enable circumvention is illegal.

What I was walling in or walling out.[147]

IV. CONCLUSION

Copyright owners are among those who will use technology as a means of controlling unauthorized access to and use of their documents in digital networked environments. This technology shows considerable promise as a way to protect the legitimate interests of copyright owners. Whether legislation to prohibit development of circumvention technologies is needed right now is a subject worthy of more debate than the drafters of the White Paper are hoping it will get. Professor Ejan MacKaay, who is an economist as well as a copyright scholar with a deep interest and appreciation of the challenges and opportunities of emerging digital networks, has suggested in a recent paper that it is simply too early to tell whether legislation is needed.[148] Let copyright owners use technology to build "fences" around their works and explore new markets. If the fences they use are inadequate to protect against market failure, there will be time enough to adopt appropriate legislation at that time. Even if policymakers decide that some anti-circumvention provision is needed now, this article has shown that serious consideration should be given to a more narrowly drawn law. The White Paper proposal is too much too soon and has potential to do a considerable amount of unintended mischief, as well as to propel copyright policy in a direction for which it is currently ill-equipped.

It is no exaggeration to say that copyright is at the cusp of a new era, one in which technology will play an important role. Before making particular policy choices about the role technology should or should not have, such as the policy choices proposed in the White Paper, we would do well to reflect on other policy options that may be open now but that may be foreclosed later if we choose to follow the path that the White Paper has charted. John Seely Brown, who is the Chief Scientist of Xerox Corp. and the head of its Palo Alto Research Center recently observed:

> Much debate tends to argue that document technologies determine certain social processes--either for good or for ill. So, for example, theorists of literacy such as Walter Ong, Marshall McLuhan, Elizabeth Eisenstein, Jack Goody, and Richard Lanham, have painted the onset of democracy and the rise of individual freedom as the inevitable and unavoidable outcome of the spread of printing or information technology. From a profoundly different perspective, Weberians, Chandlerians, and Foucauldians have linked documentary technology to the rise of social control and the increasing spread of bureaucratic-institutional power and repression.

---

[147] Frost, supra note --.

[148] Ejan MacKaay, Allocating Intellectual Property Rights in a Networked Environment: An Economic Analysis, in ACADEMY COLLOQUIUM ON THE FUTURE OF COPYRIGHT IN A DIGITAL ENVIRONMENT (Bernt Hugenholtz and Egbert Dommering, eds. forthcoming 1996).

> While document technology is undoubtedly linked to both, neither of these accounts gives the whole picture. And neither result is inevitable. As Oswyn Murray has suggested, it's more reasonable to think of technology as an enabler with the potential to support various scenarios. Which scenarios will play out (and there will undoubtedly be more than one), will be the result of a great deal of social work, conflict, coordination, and creativity, conducted around but not determined by the technology.
>
> This argument surely holds for the Internet too. Some argue it will fulfill social democratic ideals, others that it will undermine civil, political, and economic institutions. Each outcome is no doubt feasible, but the technology alone guarantees neither. The outcome of contemporary social-technological pressures for change, whether for good or for ill, will be the result of social struggle and negotiation. Consequently, the means of negotiation are particularly important. Here, the Internet and related technologies are intriguingly both the form and the topic of debate.[149]

Technology does not impel us to the policy choices that the White Paper proposes. Other possibilities may balance author, publisher and user interests more optimally than the White Paper would. These alternatives deserve more careful exploration to ensure that the choice made now is one that we and our children can live with for a long time to come.

---

[149] John Seely Brown & Paul Daguid, The Social Life of Documents, RELEASE 1.0 at 13 (Oct. 11, 1995).