

Some Reflections on Copyright Management Systems
and Laws Designed to Protect Them

(first published 12 Berkeley Tech. L.J. 161 (1997))

Julie E. Cohen *

I. Introduction	161
II. Legislative and Treaty Developments	163
A. The National Information Infrastructure Copyright Protection Act	164
B. The Geneva Connection: The WIPO Treaty	165
C. The 105th Congress: WIPO or "WIPO Plus"?	169
III. Overbreadth Concerns	172
A. Knowledge, Purpose, and Effect	172
B. "Or Permitted By Law:" Fair Use and Other Authorized Uses	175
C. Remedial Overkill	178
IV. Broader Implications of Private Copyright Management Regimes	179
A. Copyright, Contract, and "Private Legislation"	179
B. Reader Privacy and Anonymity	183
V. Conclusion	187

I. Introduction

Copyright management systems (CMS)--technologies that enable copyright owners to regulate reliably and charge automatically for access to digital works--are the wave of the very near future. The advent of digital networks, which make copying and distribution of digital content quick, easy, and undetectable, has provided the impetus for CMS research and development.¹ CMS are premised on the concept of "trusted systems" or "secure digital

*© 1997 Julie E. Cohen. Assistant Professor of Law, University of Pittsburgh School of Law. Email: cohen@law.pitt.edu. J.D. 1991, Harvard Law School. An earlier version of this paper was presented at a March 1997 conference on the WIPO Copyright Treaty co-sponsored by the American Committee for Interoperable Systems and Santa Clara University School of Law. I would like to thank the participants in that conference, in particular Peter Jaszi and Pamela Samuelson, for their thought-provoking comments, and Tom Zagorsky for research assistance.

¹See, e.g., U.S. Dep't of Commerce, Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights 10-12, 177-78, 230 (1995) [hereinafter NII White Paper]; Jon Bing, *The Contribution of Technology to the Identification of Rights, Especially in Sound and Audio-Visual Works: An Overview*, 4 Int'l. J. L. & Info. Tech. 234, 235-36 (1996); Christopher Burns, Inc., Copyright Management and the NII: Report to the Enabling Technologies Committee of the Association of American Publishers 15-16 (1996); Mark Stefik, *Letting Loose the Light: Igniting Commerce in Electronic Publication, in Internet Dreams: Archetypes, Myths, and Metaphors*

envelopes" that protect copyrighted content and allow access and subsequent copying only to the extent authorized by the copyright owner.² Software developers are testing prototype systems designed to detect, prevent, count, and levy precise charges for uses that range from downloading to excerpting to simply viewing or listening to digital works.³ In a few years, for example, an individual seeking online access to a collection of short fiction might be greeted with a menu of options including:

- Open and view short story A -- \$0.50, or \$0.40 for students doing assigned reading (verified based on roster submitted by instructor)
- Open and view short story B (by a more popular author) -- \$0.80, or \$0.70 for students
- Download short story A (encrypted and copy-protected) -- \$1.35
- Download short story B -- \$2.25
- Download entire collection -- \$15.00
- Extract excerpt from short story A -- \$0.03 per 50 words
- Extract excerpt from short story B -- \$0.06 per 50 words

CMS also loom large on the legislative horizon. Copyright owners have argued that technological protection alone will not deter unauthorized copying unless the law provides

219, 220-22 (Mark Stefik, ed., 1996) [hereinafter Stefik, *Letting Loose the Light*] ("[C]omputers need not be blind instruments of copyright infringement. Properly designed digital systems can be more powerful and flexible instruments of trade in publications than any other medium.").

²See Charles Clark, *The Publisher in the Digital World*, in INTELLECTUAL PROPERTY RIGHTS AND NEW TECHNOLOGIES: PROCEEDINGS OF THE KNOWRIGHT '95 CONFERENCE 85, 97-101 (Klaus Brunnstein & Peter Paul Sint, eds., 1995); Stefik, *supra* note 1, at 226-34; Mark Stefik, *Shifting the Possible: How Digital Property Rights Challenge Us to Rethink Digital Publishing*, 12 BERKELEY TECH. L.J. 138, 139-40 (1997) [hereinafter Stefik, *Shifting the Possible*]; International Federation of Reproduction Rights Organizations, Committee on New Technologies, *Digital Rights Management Technologies*, (visited April 17, 1997) <http://www.ncri.com/articles/rights_management/> [hereinafter IFRRO Report].

³See Bing, *supra* note 1, at 261-66; Burns, *supra* note 1, at 17-21, 30-35; Clark, *supra* note 2, at 97-101; Stefik, *Shifting the Possible*, *supra* note 2, at 142; IFRRO Report, *supra* note 2.

penalties for circumventing the technology.⁴ Although a bill to protect CMS against tampering failed to reach a vote in Congress last year, the World Intellectual Property Organization's recent adoption of treaty provisions requiring protection means that Congress must revisit the question soon. Part II describes these developments.

The seemingly inexorable trend toward a digital CMS regime raises two questions, which I address in parts III and IV, respectively. First, broadly drawn protection for CMS has the potential to proscribe technologies that have indisputably lawful uses and also to foreclose, as a practical matter, uses of copyrighted works that copyright law expressly permits. How may protection for CMS be drafted to avoid disrupting the current copyright balance? Second, and equally fundamental, CMS may enable both pervasive monitoring of individual reading activity and comprehensive "private legislation" designed to augment--and possibly alter beyond recognition--the default rules that define and delimit copyright owners' rights. Given the unprecedented capabilities of these technologies, is it also desirable to set limits on their reach?

II. Legislative and Treaty Developments

Emerging schemes for legislative protection of CMS have two components. First, they prohibit tampering with protective technologies adopted by copyright owners. Second, they prohibit the unauthorized removal or alteration of so-called "rights management information" (RMI) attached to copies of copyrighted works. Because RMI is defined to include the terms and conditions for use of the work, tampering with CMS (which enforce terms and conditions) may constitute an RMI violation, and vice versa.

The following three subsections lay out the various legislative proposals and treaty provisions that are likely to shape the domestic debate over CMS and RMI.

A. The National Information Infrastructure Copyright Protection Act

In 1995, the Clinton Administration's Information Infrastructure Task Force released a "White Paper" on "Intellectual Property and the National Information Infrastructure," which

⁴See, e.g., *National Information Infrastructure: Hearing on S. 1284 Before the Senate Comm. on the Judiciary*, 104th Cong. (May 7, 1996) (testimony of Kenneth R. Kay, Executive Director, Creative Incentive Coalition), available in WESTLAW, USTestimony database; *Copyright Protection on the Internet: Hearings on H.R. 2441 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 104th Cong. (Feb. 7-8, 1996) (statements on Feb. 7, 1996 of Barbara A. Munder, Senior Vice President, The McGraw-Hill Companies, Inc.; Frances W. Preston, President and CEO, Broadcast Music, Inc.; Jack Valenti, Chairman and Chief Executive Officer, Motion Picture Association of America, Inc.; and statement on Feb. 8, 1996 of the Association of American Publishers), available in WESTLAW, USTestimony database; see also NII White Paper, supra note 1, at 230 (endorsing anti-tampering legislation for that reason).

included recommended changes to the Copyright Act to address perceived difficulties concerning the Act's application to digital works.⁵ The National Information Infrastructure Copyright Protection Act (NIICPA), a verbatim rendering of the White Paper's proposals, was introduced in Congress in the fall of 1995.⁶ However, the NIICPA's provisions engendered strong opposition from a variety of groups, including educators, librarians, Internet service providers, and manufacturers of consumer electronic equipment.⁷ As a result, the bill remained stalled in committee when the 104th Congress adjourned. Of particular importance for this discussion, the NIICPA includes a proposed Chapter 12 for the Copyright Act, which was designed to protect CMS.

1. Technological Protection

The anti-circumvention provision, proposed section 1201 of the Copyright Act, reads as follows:

Section 1201. Circumvention of copyright protection systems.

No person shall import, manufacture, or distribute any device, product, or component incorporated into a device or product, or offer or perform any service, 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

2. Rights Management Information

Proposed section 1202 of the Copyright Act would provide protection for RMI:

Section 1202. Integrity of copyright management information.

(a) False Copyright Management Information--No person shall knowingly provide copyright management information that is false, or knowingly publicly distribute or import for public distribution copyright management information that is false.

⁵NII White Paper, *supra* note 1.

⁶National Information Infrastructure Copyright Protection Act, S. 1284 & H.R. 2441, 104th Cong. (1995) [hereinafter NIICPA].

⁷See Digital Future Coalition, collected position statements, letters, and press releases (visited April 5, 1997) <<http://www.ari.net/dfc/>>.

⁸NIICPA, *supra* note 6, at § 4 (proposed § 1201 of the Copyright Act).

(b) Removal or Alteration of Copyright Management Information--No person shall, without authority of the copyright owner or the law, (i) knowingly remove or alter any copyright management information, (ii) knowingly distribute or import for distribution copyright management information that has been altered without authority of the copyright owner or the law, or (iii) knowingly distribute or import for distribution copies or phonorecords from which copyright management information has been removed without authority of the copyright owner or the law.

(c) Definition--As used in this chapter, 'copyright management information' means the name and other identifying information of the author of a work, the name and other identifying information of the copyright owner, terms and conditions for uses of the work, and such other information as the Register of Copyrights may prescribe by regulation.⁹

3. Remedies and Defenses

The NIICPA would authorize a panoply of civil remedies for violation of sections 1201 and/or 1202. Monetary remedies available to the copyright owner include "damages suffered . . . as a result of the violation, and any profits of the violator that are attributable to the violation and are not taken into account in computing the actual damages,"¹⁰ statutory damages up to \$2,500 per violation of section 1201 and \$25,000 per violation of section 1202,¹¹ treble damages for repeated violations,¹² and costs and attorneys' fees.¹³

In addition, the remedial provisions would allow courts to impound "any device or product that is in the custody or control of the alleged violator and that the court has reasonable cause to believe was involved in a violation."¹⁴ After final judgment, the court could order the device or product destroyed.¹⁵

⁹*Id.* § 1202.

¹⁰*Id.* § 1203(c)(2).

¹¹*Id.* § 1203(c)(3).

¹²*Id.* § 1203(c)(4).

¹³*Id.* § 1203(b)(4)-(5).

¹⁴*Id.* § 1203(b)(2).

¹⁵*Id.* § 1203(b)(6).

Finally, the NIICPA would authorize criminal penalties against persons violating section 1202 "with intent to defraud."¹⁶

B. The Geneva Connection: The WIPO Treaty

In December 1996, delegates to the World Intellectual Property Organization (WIPO) met in Geneva to craft a protocol to the Berne Convention regarding copyright in digital works. Notwithstanding the Clinton Administration's failure to generate domestic consensus behind the NIICPA, the United States proposal to WIPO substantially tracked the language of the NIICPA.¹⁷ With respect to CMS, however, the treaty provisions ultimately adopted differ considerably from those initially urged by the United States government.

1. Technological Protection

The anti-tampering provision originally proposed by Jukka Liedes, Chairman of the Committees of Experts (proposed Article 13) reads as follows:

Article 13: Obligations concerning Technological Measures

(1) Contracting Parties shall make unlawful the importation, manufacture or distribution of protection-defeating devices, or the offer or performance of any service having the same effect, by any person knowing or having reasonable grounds to know that the device or service will be used for, or in the course of, the exercise of rights provided under this Treaty that is not authorized by the rightholder or the law.

(2) Contracting Parties shall provide for appropriate and effective remedies against the unlawful acts referred to in paragraph (1).

(3) As used in this Article, "protection-defeating device" means any device, product or component incorporated into a device or product, the primary purpose or primary effect

¹⁶*Id.* § 1204.

¹⁷U.S. Department of Commerce, Protocol to the Berne Convention for the Protection of Literary and Artistic Works (*proposed*), Submitted to Committees of Experts by Bruce Lehman, Ass't Sec. of Commerce and Commissioner of Patents and Trademarks, November 29, 1995 (on file with author); see Pamela Samuelson, *Big Media Beaten Back*, *Wired*, Mar. 1997, at 61, 62-64 (quoting statement by Bruce Lehman, chair of the working group that produced the NII White Paper and head of the United States delegation to WIPO, that characterized the treaty process as "a second bite at the apple").

of which is to circumvent any process, treatment, mechanism or system that prevents or inhibits any of the acts covered by the rights under this Treaty.¹⁸

In accompanying comments, Chairman Liedes conceded that the proposed requirements were "more akin to public law obligations . . . than to provisions granting 'intellectual property rights.'"¹⁹ He indicated that in implementing the proposal, parties should consider "the need to avoid legislation that would impede lawful practices and the lawful use of subject matter that is in the public domain."²⁰ However, he maintained that a primary-purpose-or-effect standard for identifying unlawful devices, rather than a narrower focus on devices "specifically designed or adapted to circumvent" technological protection, was the only way "[t]o achieve the necessary coverage."²¹

The primary-purpose-or-effect language met with considerable resistance. Many delegates expressed concern that the provision might restrict access to public domain materials and frustrate lawful uses of copyrighted works, such as fair use.²² Several delegates also expressed concern that the provision as worded would reach a variety of devices capable of substantial and valuable noninfringing uses.²³ As finally approved by the delegates, the provision (now Article 11), is substantially altered:

Article 11: Obligations concerning Technological Measures

¹⁸World Intellectual Property Organization, Chairman of the Committees of Experts on a Possible Protocol to the Berne Convention and on a Possible Instrument for the Protection of the Rights of Performers and Producers of Phonograms, Basic Proposal for the Substantive Provisions of the Treaty on Certain Questions Concerning the Protection of Literary and Artistic Works to be Considered by the Diplomatic Conference, Art. 13 (Aug. 30, 1996) [hereinafter WIPO Basic Proposal].

¹⁹*Id.* Art. 13, cmt. 13.03.

²⁰*Id.* Art. 13, cmt. 13.05.

²¹*Id.* Art. 13, cmt. 13.06.

²²Seth Greenstein, *News from WIPO: Day Seven--The Audio Visual Debate, and What's Fair Is Fair Use* (visited Apr. 5, 1997) <http://www.hrrc.org/wr_12-10.html> (reporting comments by delegates).

²³*Id.*; John Browning, *Africa 1 Hollywood 0*, *Wired*, Mar. 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.").

Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.²⁴

The new language focuses on the need for protection against the act of circumventing CMS, rather than the nature of the device used to accomplish circumvention.

2. *Rights Management Information*

Initially, the proposed treaty provision regarding RMI (proposed Article 14) read as follows:

Article 14: Obligations concerning Rights Management Information

(1) Contracting Parties shall make it unlawful for any person knowingly to perform any of the following acts:

(i) to remove or alter any electronic rights management information without authority;

(ii) to distribute, import for distribution or communicate to the public, without authority, copies of works from which electronic rights management information has been removed or altered without authority.

(2) As used in this Article, "rights management information" means information which identifies the work, the author of the work, the owner of any right in the work, and any numbers or codes that represent such information, when any of these items of information are attached to a copy of a work or appear in connection with the communication of a work to the public.²⁵

²⁴World Intellectual Property Organization, Provisional Treaty on Protection of Literary and Artistic Works, Art. 11, 53 Pat. Trademark & Copyright J. 155, 156 (1997) [hereinafter *WIPO Provisional Treaty*]. This language was drafted by the African delegates, who emerged during the negotiations as a critical, and thoughtful, voting bloc. See Browning, *supra* note 23, at 186.

²⁵WIPO Basic Proposal, *supra* note 18, Art. 14.

Once again, the comments of Chairman Liedes stressed "the need to avoid legislation that would impede lawful practices,"²⁶ or that would impose "technically non-feasible requirements" on broadcasters and other authorized users.²⁷

After many delegates requested that the RMI provision be modified to require some connection to infringing purpose,²⁸ the provision (now Article 12) was redrafted as follows (changes underlined):

Article 12: Obligations concerning Rights Management Information

(1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing or, with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention:

(i) to remove or alter any electronic rights management information without authority;

(ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.

(2) As used in this Article, "rights management information" means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public.²⁹

As revised, this provision requires not only knowing performance of a prohibited act, but also knowledge (or at least reasonable basis for knowledge) that the act will facilitate an act of copyright infringement. In addition, liability for distribution of altered works is imposed only if the distributor also knows that RMI was removed without authority.

²⁶*Id.* Art. 14, cmt. 14.04.

²⁷*Id.* Art. 14, cmt. 14.05.

²⁸*See* Greenstein, *supra* note 22.

²⁹*WIPO Provisional Treaty, supra* note 24, Art. 12, at 156.

However, the scope of Article 12 was broadened in one crucial respect. The definition of RMI was expanded to include information about the terms and conditions set by the owner for use of the work, as well as "numbers or codes that represent such information." As noted above, because CMS necessarily incorporate this information, a single act of tampering may implicate both Article 12 and Article 11.

C. The 105th Congress: WIPO or "WIPO Plus"?

As of this writing, no bill implementing the provisions of the new WIPO copyright treaty has been introduced in either house of Congress. Many of the new treaty provisions would require little or no change to existing United States law.³⁰ However, at least some of the provisions concerning CMS will require implementing legislation if Congress ratifies the treaty.³¹

Articles 11 and 12 of the WIPO copyright treaty leave substantial room for variation in the implementing legislation crafted by member states. Of particular significance for the United States, the provisions require merely a threshold level of protection and do not prohibit member states from adopting stricter laws, such as the anti-tampering provisions of the NIICPA. In a

³⁰This appears to be the consensus view. See Samuelson, *supra* note 17, at 180; *Clinton Administration is Undecided on Implementing Steps for WIPO Treaties*, 53 Pat. Trademark & Copyright J. 241, 242 (1997) [hereinafter *Implementing WIPO Treaties*].

³¹According to Prof. Samuelson, implementing legislation would be necessary only for Article 12, regarding RMI. Samuelson, *supra* note 17, at 180. Article 12 defines RMI to include "information which identifies the work, the author of the work, the owner of any right in the work, or information about terms and conditions of use of the work . . ." *WIPO Provisional Treaty*, *supra* note 24, at 156. Removal or alteration of the first three items would be actionable under § 43(a) of the Lanham Act, which prohibits the use in commerce of "any false designation of origin, false or misleading description of fact, or false or misleading representation of fact" that is likely to confuse consumers as to the origin or sponsorship of a product or service. 15 U.S.C.A. § 1125(a)(1) (West, WESTLAW through P.L. 105-4, approved Mar. 3, 1997). However, § 43(a) does not appear to cover removal of information about terms and conditions of use.

As to Article 11, Prof. Samuelson believes that the doctrine of contributory copyright infringement already provides the required "adequate and effective" remedy against circumvention of CMS. Conversation with Pamela Samuelson, Law Professor, Univ. of Cal. at Berkeley (Mar. 14, 1997). The doctrine extends infringement liability to knowing purveyors of technologies that have no "substantial noninfringing use." *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 441-42 (1984); *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 264 (9th Cir. 1996); *Casella v. Morris*, 820 F.2d 362, 365 (11th Cir. 1987); *Gershwin Pub. Corp. v. Columbia Artists Management, Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971). For the reasons discussed in part III.B, *infra*, I do not believe that the "substantial noninfringing use" doctrine alone can resolve the problem of tampering with CMS.

recent briefing, PTO Commissioner Bruce Lehman indicated that the Administration will attempt to seek passage of the NIICPA in the 105th Congress.³² However, it is unclear whether the Administration will stand firm behind the precise language that failed to generate consensus last year in Congress and again in Geneva. One possible source for new language is a draft committee print of revisions to the NIICPA that was circulated before Congress adjourned last summer.³³

1. Technological Protection

Although arguably less draconian than the original proposal, the draft language would impose significantly higher levels of protection for CMS than the treaty language requires (changes to the original NIICPA language are underlined):

Section 1201. Circumvention of copyright protection systems.

(a) Prohibitions--No person shall import, manufacture, or distribute any device, product, or component incorporated into a device or product, or offer or perform any service, an effect of which is to avoid, bypass, remove, deactivate or otherwise circumvent [. . .] any process, treatment, mechanism, or system which prevents or inhibits the infringement of any of the exclusive rights of the copyright owner under section 106, with reckless disregard for facts demonstrating that the device, product, component, or service primarily enables such infringement, or with the intent to primarily enable such infringement.

(b) Limitation--Liability under this section shall not be based solely upon the failure of a device, product, or service to accommodate, facilitate, or enable the operation of any process, treatment, mechanism, or system described in subsection (a).³⁴

2. Rights Management Information

Section 1202 of the draft committee print is very similar to the final WIPO treaty provision on RMI (changes to the original NIICPA language are underlined):

Section 1202. Integrity of copyright management information.

³²*Implementing WIPO Treaties, supra* note 30, at 242.

³³Staff of House Subcomm. on Courts and Intellectual Property, 104th Cong., NII Copyright Protection Act of 1995, H.R. 2441 § 106 (Draft Comm. Print 1996) (on file with author) [hereinafter NIICPA Draft Committee Print].

³⁴*Id.* § 1201.

(a) False Copyright Management Information--No person shall knowingly provide copyright management information that is false, or knowingly publicly distribute or import for public distribution copyright management information that is false, with intent to mislead or to induce or facilitate infringement.

(b) Removal or Alteration of Copyright Management Information--No person shall, without authority of the copyright owner or other lawful authority, knowingly and with intent to mislead or to induce or facilitate infringement--

(1) remove or alter any copyright management information,

(2) distribute or import for distribution copyright management information that has been altered without authority of the copyright owner or other lawful authority, or

(3) distribute or import for distribution copies or phonorecords from which copyright management information has been removed without authority of the copyright owner or other lawful authority.

(c) Definition--As used in this chapter, the term 'copyright management information' means the following information that appears in connection with copies or phonorecords of a work or performances or displays of a work, including in digital form:

(1) The title and other information identifying the work, including the information set forth in a notice of copyright.

(2) The name and other identifying information of the author of the work.

(3) The name and other identifying information of the copyright owner of the work, including the information set forth in a notice of copyright.

(4) Terms and conditions for uses of the work.

(5) Identifying numbers or symbols referring to such information.

(4) [sic] Such other information as the Register of Copyrights may prescribe by regulation.³⁵

3. Remedies and Defenses

³⁵*Id.* § 1202.

In the draft committee print of the NIICPA, the civil remedial provision is modified to afford a defense where the offending device, product, or component "was generally available in the relevant market prior to the introduction into that market of the process, treatment, mechanism, or system circumvented."³⁶

The provision creating criminal liability, however, is enlarged to reach violations of section 1201 "with intent to infringe upon any of the exclusive rights of the copyright owner under section 106," as well as violations of section 1202 "with intent to defraud."³⁷ This language is substantially broader than required by the WIPO treaty. On its face, the treaty does not require criminal penalties at all, but only "adequate and effective legal remedies" for the copyright owner.³⁸

III. Overbreadth Concerns

Legislating permissible developments in computer technology is a dangerous project. Invariably, technologies that might be used for indisputably unlawful purposes are the same technologies that are useful for achieving many lawful and socially valuable ones. Devices or services that might be used to defeat CMS are a case in point.

Article 11 of the WIPO copyright treaty is scrupulously attentive to this problem. It focuses on conduct in particular cases--circumvention of CMS designed to restrict unauthorized, infringing acts--and does not attempt to define a class of technologies that should be prohibited. In contrast, the NIICPA and its proponents have at best ignored, and at worst denied, the undeniable fact that "effects" legislation threatens lawful and socially valuable conduct.

A. Knowledge, Purpose, and Effect

Under the NIICPA, a finding of liability for tampering hinges on two factors. First, the accused technology is classified according to its effect in general, rather than its use to achieve infringement in a specific case. As originally worded, section 1201 of the NIICPA targets any technology or service with the "primary purpose or effect" of defeating CMS.³⁹ The draft committee version goes even farther, extending liability to any technology or service "an effect of

³⁶*Id.* § 1203(d).

³⁷*Id.* § 1204(a)-(b).

³⁸*WIPO Provisional Treaty, supra* note 24, at 156.

³⁹NIICPA, *supra* note 6, § 1201.

which" is to defeat CMS.⁴⁰ Second, the defendant's conduct must be knowing--but sections 1201 and 1202 of the NIICPA, as originally worded, require knowledge only as to the acts that constitute tampering, not as to any ultimate act of infringement.⁴¹

The primary-purpose-or-effect test is a radical departure from existing copyright law, in two distinct ways. First, copyright law treats with suspicion blanket prohibitions on technologies that are merely capable of facilitating infringement. Thus, a claim for contributory copyright infringement fails as a matter of law if the accused device is capable of substantial noninfringing use.⁴² In *Sony Corp. of America v. Universal City Studios, Inc.*, the Supreme Court noted that in the context of patent law, "a finding of contributory infringement is normally the functional equivalent of holding that the disputed article is within the monopoly granted to the patentee."⁴³ The Court reasoned that in copyright law, a "substantial noninfringing use" standard would similarly "strike a balance between a copyright holder's legitimate demand for effective--not merely symbolic--protection . . . and the rights of others freely to engage in substantially unrelated areas of commerce."⁴⁴ This reasoning applies equally to technologies that might potentially play a role in defeating CMS. Such technologies include encryption and decryption tools, which are considered crucial to the development of Internet-based commerce;⁴⁵ tools for software reverse engineering, which have widespread lawful application and are protected by the fair use doctrine;⁴⁶ and possibly even that most ubiquitous hacking tool, the personal computer.⁴⁷

⁴⁰NIICPA Draft Committee Print, *supra* note 33, § 1201(a) (emphasis added).

⁴¹*See* NIICPA, *supra* note 6, §§ 1201-02. The draft committee version tightens this standard slightly, but not far enough. *See* text accompanying notes 54-55, *infra*.

⁴²*See* *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 440-41 (1984).

⁴³*Id.* at 441.

⁴⁴*Id.* at 442.

⁴⁵*See*, e.g., David Chaum, *Achieving Electronic Privacy*, *Sci. Am.*, Aug. 1992, at 96, 96-97 (visited Apr. 26, 1997) <<http://ganges.cs.tcd.ie/mepeirce/Project/Chaum/sciam.html>>; A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 *J.L. & Com.* 395, 453-71 (1996).

⁴⁶*See* *Sega Enterprises, Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1521-28 (9th Cir. 1992); *DSC Communications Corp. v. DGI Technologies, Inc.*, 898 F. Supp. 1183, 1188-91 (N.D. Tex. 1995), *aff'd on other grounds*, 81 F.3d 597 (5th Cir. 1996); Julie E. Cohen, *Reverse Engineering and the Rise of Electronic Vigilantism: Intellectual Property Implications of "Lock-Out" Programs*, 68 *S. Cal. L. Rev.* 1091, 1104-34 (1995) [hereinafter Cohen, *Reverse Engineering*].

⁴⁷*See* Browning, *supra* note 23, at 186 (noting objections to proposed Article 13 of the WIPO treaty on this basis).

Giving copyright owners control over this broad spectrum of technological capability is bad policy, and likely to prove unworkable in practice.

Congress has historically dealt with perceived technological threats to copyright owners' rights by enacting narrow, targeted pieces of legislation. Thus, the Audio Home Recording Act requires digital recording devices to incorporate serial copy management technology,⁴⁸ and the Communications Act regulates devices for decrypting satellite broadcasts.⁴⁹ As Thomas Vinje has pointed out, both pieces of legislation address specific technologies that have few other markets and are unlikely to be deployed unintentionally.⁵⁰ Along similar lines, some commentators (including a number of delegates to the WIPO convention) have proposed that anti-tampering laws ban only devices designed with the "sole intended purpose" of defeating CMS.⁵¹ Like the contributory infringement standard, a "sole intended purpose" test would help to minimize the NIICPA's effect on technologies capable of a diverse range of application. Neither standard, however, addresses the second major problem that the NIICPA would create for existing copyright law.

The second way in which the NIICPA departs from existing copyright law is in its failure to recognize that some instances of tampering with CMS may be necessary to preserve the public's current rights. For example, readers may wish to make fair use of copyrighted works, or to copy works that are in the public domain. As a practical matter, both the "no substantial noninfringing use" and "sole intended purpose" tests would hinder such efforts. If a device or service satisfied either standard, it could be banned outright--even though it might also be used to facilitate "lawful tampering." Alternatively, lawful tampering might be defined as a substantial noninfringing use--with the result that the sale or importation of a circumvention device would never, or hardly ever, trigger liability. This result is appealing, but unlikely to be what the drafters of the NIICPA had in mind.

⁴⁸17 U.S.C. § 1002(c) (1994).

⁴⁹47 U.S.C.A. § 605(e)(4) (West, WESTLAW through Nov. 1996).

⁵⁰Thomas C. Vinje, *A Brave New World of Technical Protection Systems: Will There Still Be Room for Copyright?*, 8 Eur. Intell. Prop. Rev. 431, 433 (1996).

⁵¹*See, e.g.*, Greenstein, *supra* note 22 (reporting on proposals made during the WIPO Diplomatic Conference by the African Group--Burkina Faso, Cameroon, Cote d'Ivoire, Egypt, Ghana, Kenya, Malawi, Namibia, Nigeria, Rwanda, Senegal, Sudan, Togo, Tunisia, and Zambia--and by Singapore); Vinje, *supra* note 50, at 435. The European Community's directive on the legal protection of computer software, which contains a provision regarding circumvention of devices used to protect computer programs, employs a "sole intended purpose" test. *See* Council Directive 91/250/EEC of 14 May 1991 on the Legal Protection of Computer Programs, art. 7(c), 1991 O.J. (L 122) 42.

The concept of "lawful tampering" is considered more fully below. I raise it here only to show that the delegates to the WIPO convention were correct in concluding that liability under an anti-tampering statute should hinge on something more than a technology's capabilities. For example, the statute might focus on the tamperer's (as opposed to the technology's) purposes. The knowledge requirements in proposed sections 1201 and 1202 of the NIICPA, however, merely contribute to the likelihood that the anti-tampering provisions might be used to suppress valuable technologies and lawful uses. As originally worded, both sections would require only knowing use of the challenged technology, not knowing infringement.

There is, of course, strict liability for copyright infringement.⁵² As Chairman Lides noted in his comments to the draft WIPO treaty, however, anti-tampering provisions do not establish intellectual property rights, but merely create a general class of obligations toward copyright owners who adopt technological measures to protect their works.⁵³ Given the need to preserve existing public rights of access, importing strict liability into these ancillary enforcement provisions would be unwise. Consider, for example, an individual who tampers with CMS to enable a use that she believes is fair. Her acts of tampering are knowing, but she lacks intent to infringe; indeed, she affirmatively intends not to infringe. If her beliefs regarding fair use prove mistaken, she will be held liable for infringement. Subjecting her to liability for tampering as well seems both unfair and unnecessary. The scope of the fair use doctrine is uncertain enough to force would-be fair users to think carefully. Strict liability seems advisable only if one believes that the law should provide additional disincentives to those wishing to exercise fair use rights.

The draft revisions to section 1202 of the NIICPA are a step in the right direction. The new language would require both that the conduct be knowing and that the defendant possess "intent to mislead or to induce or facilitate infringement."⁵⁴ The revisions to section 1201 are less satisfactory; they require either "intent to primarily enable . . . infringement" or "reckless disregard" for facts showing that the device "primarily enables" infringement.⁵⁵ The latter requirement is simply a nonspecific "effects" test restated in terms of the evidence needed to meet it. Instead, section 1201 should be redrafted to eliminate the "effects" test and to include the same strict knowledge standard contained in the revised section 1202.

B. "Or Permitted By Law:" Fair Use and Other Authorized Uses

⁵²See 17 U.S.C. § 501(a) (1994).

⁵³See WIPO Basic Proposal, *supra* note 18, Art. 13, cmt. 13.03.

⁵⁴NIICPA Draft Committee Print, *supra* note 33, § 1202(a).

⁵⁵*Id.* § 1201(a).

As noted above, the task of drafting effective, appropriately tailored anti-tampering legislation is complicated by the fact that unauthorized use of a copyrighted work is not always infringement. In consequence, CMS that prevent (for example) all copying, or all free copying, will almost certainly frustrate some actions that the Copyright Act would permit. Lawmakers should therefore consider whether and to what extent an anti-tampering law should protect CMS that have this effect.

The Copyright Act does not entitle copyright owners to control all uses of their copyrighted works. Instead, it gives them the exclusive right to perform or authorize the six acts listed in section 106: reproduction, preparation of derivative works, distribution, performance, display, and (for sound recordings) digital performance.⁵⁶ In addition, the Act provides a number of exceptions to these exclusive rights for particular uses and/or users. The most well known is section 107, which codifies the fair use doctrine.⁵⁷ Others include the provision allowing libraries to reproduce and distribute single copies of works for research and archival purposes,⁵⁸ and the provision allowing certain types of nonprofit performances and displays.⁵⁹

Moreover, many works that might be made available in digital form are wholly unprotected by copyright. In some cases, the term of copyright protection has expired and the work has entered the public domain. Other works are ineligible for copyright protection in the first place, because they fail to satisfy the originality requirement set forth in *Feist Publications, Inc. v. Rural Telephone Service Co.*⁶⁰

Article 11 of the WIPO treaty requires member nations to protect against the circumvention of CMS "that restrict acts . . . which are not authorized by the authors concerned or permitted by law."⁶¹ Section 1201 of the NIICPA similarly prohibits technologies that operate to circumvent CMS "without the authority of the copyright owner or the law."⁶² According to the Clinton Administration's White Paper, this language is sufficient to preserve fair use and access to public

⁵⁶17 U.S.C. § 106 (1994).

⁵⁷*See id.* § 107 (1994).

⁵⁸*See id.* § 108 (1994).

⁵⁹*See id.* § 110 (1994).

⁶⁰499 U.S. 340, 347-50 (1991) (requiring originality in "selection or arrangement" of data in order for a compilation to gain copyright protection).

⁶¹*WIPO Provisional Treaty, supra* note 24, Art. 11, at 156.

⁶²NIICPA, *supra* note 6, § 1201.

domain materials.⁶³ However, the White Paper does not indicate how this preservation is to be accomplished. In fact, the problem is quite difficult, because works placed under technological protection are materially less accessible than before.

Taken literally, the language of Article 11 could be read to suggest no obligation to protect systems that restrict lawful acts. Thus, one solution might be to require that to be eligible for protection, CMS be designed to allow any uses of the underlying works that would be lawful. Realistically, however, this is unlikely to happen. First, copyright owners and other content providers welcome digital CMS precisely because of their capacity to define and enforce "usage rights" in digital works by electronic contract.⁶⁴ The White Paper expressly approves this possibility.⁶⁵ For noncopyrightable factual compilations, contract is currently the only way of ensuring that vendors can recoup their development costs.⁶⁶ Whether an anti-tampering law would or should shield the use of contract as a supplement to copyright is considered further in part IV.A, *infra*. Second, and more important, even if copyright owners were willing (or required) to design their systems to allow for fair use, library copying, and the like, designing around the fair use doctrine may be a near-impossible task. Automated CMS are inherently ill-equipped to handle the equitable, fact-specific inquiry required in fair use cases.⁶⁷

⁶³See NII White Paper, *supra* note 2, at 231-32 (noting that proposed legislation targets circumvention "without authority" and that the applicable "authority" may be the author's permission or limitations upon the author's rights under the Copyright Act).

⁶⁴See, e.g., Burns, *supra* note 1, at 17-21, 29-36; Clark, *supra* note 2, at 99; Carol Risher, Libraries, Copyright and the Electronic Environment, Position Paper on Behalf of the International Publishers Copyright Council on the Occasion of the IPA 25th Congress, Barcelona, April 1996 (visited Apr. 5, 1997) <http://www.ipa-uie.org/ipcc_bcn.html>; see also Stefik, Shifting the Possible, *supra* note 2, at 147-49.

⁶⁵NII White Paper, *supra* note 2, at 58, 191-92.

⁶⁶See J.H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 Vand. L. Rev. 51, 66-69, 137-63 (1997) (noting the vulnerability of noncopyrightable information products to appropriation by others, and arguing for the creation of a new intellectual property paradigm designed to balance the competing considerations of incentives to innovate and public access to information); J.H. Reichman, *Charting the Collapse of the Patent-Copyright Dichotomy: Premises for a Restructured International Intellectual Property System*, 13 Cardozo Arts & Ent. L.J. 475, 517-20 (1995) (same).

⁶⁷Regarding the "equitable rule of reason" that governs in fair use cases, see H.R. Rep. 94-1476, at 65-66, reprinted in 1976 U.S.C.C.A.N. 5659, 5678; *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 577-78 (1994).

Mark Stefik's work belies my skepticism--but only to a degree.⁶⁸ For example, Stefik has suggested that CMS could be designed to preserve the "transfer right" afforded members of the public by the first sale doctrine.⁶⁹ His counterparts in the publishing industry, however, appear concerned solely with maximizing their control over digital content. A report commissioned by the Association of American Publishers discusses Stefik's proposal without even considering the possibility that consumers might be given the free transfer rights they enjoy in print media--and then criticizes even a fee-based system of transfer rights on the ground that "[r]ights and prices cannot be reconsidered and the publisher loses the opportunity to review the context and usage of the material proposed."⁷⁰ Moreover, even Stefik appears to envision replacing the current system of fair use and library copying with a wholly fee-based regime.⁷¹

In short, even on the unlikely assumption that copyright owners will design their CMS with the public interest in mind, it is virtually certain that CMS adopted to protect digital works will prevent some actions that copyright law allows. Members of the public will be able to take these allowable actions only to the extent that they can defeat the system of technological protection surrounding the work. Thus, we come to the question of "lawful tampering."

Lawful tampering seems to be the solution contemplated by the drafters of the NII White Paper--yet here the White Paper is disingenuous. As discussed above, technologies for defeating CMS do not differentiate among the various lawful and unlawful uses. Thus, banning technologies that have the "effect" of circumventing CMS would leave the public free to exercise its rights of access in principle only.⁷² If the public is to have these rights in practice,

⁶⁸See Stefik, *Shifting the Possible*, *supra* note 2, at 156 (observing that the "stakeholders in digital property" include consumers and librarians).

⁶⁹17 U.S.C. § 109(a) (1994); Stefik, *Shifting the Possible*, *supra* note 2, at 145-46; *see also id.* at 152-53 (noting that CMS could be designed to release digital works when the term of copyright expires).

⁷⁰See Burns, *supra* note 1, at 34-35; *see also id.* at 16 (noting that CMS "might be resisted by users who . . . get no benefit from" them, without acknowledging that "users"--i.e., the public--may suffer any losses other than "functional disadvantages" and "complexity").

⁷¹See Stefik, *Shifting the Possible*, *supra* note 2, at 149.

⁷²The White Paper observes that "the fair use doctrine does not require a copyright owner to allow or to facilitate unauthorized access or use of a work." NII White Paper, *supra* note 1, at 231. This formulation avoids (or perhaps evades) the real question: whether copyright owners may obstruct lawful access or use of a work. For more discussion of this point, *see* Niva Elkin-Koren, *Copyright Policy and the Limits of Freedom of Contract*, 12 Berkeley Tech. L.J. 93, 111-12 (1997).

circumvention technologies may not be banned based on their capabilities alone. The law must then decide how to treat individuals who break into CMS with innocent intent.

Can tampering with CMS be made unlawful even if the act the tampering enables is lawful? Certainly. (Arguably, existing general-purpose federal statutes that prohibit tampering with information stored on someone else's computer would apply in cases of "lawful tampering"--another result that a better-designed NIICPA would prevent.⁷³ Should it? Of course not. Copyright owners cannot be prohibited from making access to their works more difficult, but they should not be allowed to prevent others from hacking around their technological barriers. Otherwise, the mere act of encoding a work within CMS would magically confer upon vendors greater rights against the general public than copyright allows.⁷⁴

C. Remedial Overkill

The NIICPA's substantive provisions are equaled in overbreadth by its civil remedial provisions. Subsections 1203(b)(2) and (b)(6), which authorize the seizure and eventual destruction of devices used to defeat CMS, are broad enough to extend to the computers used to accomplish the violations, regardless of the fact that the computers might be used for many other lawful activities.⁷⁵

Other remedial provisions are disturbingly vague. Subsection 1203(c)(2), which allows the copyright owner to recover damages and profits attributable to the violation, appears to operate as a penalty over and above damages and profits attributable to the act of copyright infringement.⁷⁶ The NIICPA does not specify how such damages might be measured, and it is difficult to think of any reliable measure. Similarly, section 1204(a) tells us that criminal

⁷³See 18 U.S.C.A. §§ 1030(a)(5), 2701 (West, WESTLAW current through P.L. 104-333, approved Nov. 12, 1996).

⁷⁴I am indebted to Professor Larry Lessig of The University of Chicago Law School for naming this proposition the "Cohen Theorem." Electronic mail from Larry Lessig to recipients of list CO-E-CONF (Nov. 11, 1996) (proceedings of 25-person online focus group convened by the United States Copyright Office, as part of its "Project Looking Forward," to discuss the future course of Internet technology and its implications for copyright) (on file with author).

⁷⁵NIICPA, *supra* note 6, §§ 1203(b)(2), (b)(6).

⁷⁶*Id.* §§ 1203(c)(2); see Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 Conn. L. Rev. 981, 991 (1996) [hereinafter Cohen, *Right to Read Anonymously*].

penalties will attach to a violation of § 1202 "with intent to defraud."⁷⁷ Since the law already provides criminal penalties for willful copyright infringement, it is unclear what the tamperer must have intended to defraud the copyright owner of in order to trigger liability under the proposed statute.⁷⁸

IV. Broader Implications of Private Copyright Management Regimes

Although the potential reach of the proposed anti-tampering provisions is troubling, even more troubling is the fact that the capabilities of CMS themselves have received so little public scrutiny.⁷⁹ As the discussion above suggests, CMS could enable private content-control regimes in which contract entirely supplants copyright as the means of mediating public access to and use of creative and informational works. In addition, because the concept of "copyright management" is predicated on the ability to generate and maintain records of the "usage rights" granted to readers, viewers, and listeners of digital works, CMS pose an enormous threat to the privacy of individual reading, viewing, and listening habits.

A. Copyright, Contract, and "Private Legislation"

The discussion of "lawful tampering" raised, but did not pursue, the question whether anti-tampering laws may be deployed in the service of copyright owners who seek to supplement their rights under the Copyright Act by enforcing contractual restrictions on the use of copyrighted works. In fact, this is the direction in which CMS are most likely headed. Even the term "copyright management" is becoming obsolete. CMS developers prefer the term "rights management," which reflects a conception of allowable authors' rights that extends beyond copyright.⁸⁰

If the "authority of . . . the law" mentioned in §§ 1201 and 1202 of the NIICPA includes contract law as well as copyright law, fewer instances of tampering may be excused as lawful.⁸¹ (The NII White Paper's deliberate lack of concern for the practical difficulties that attend unauthorized but lawful uses of works under a CMS regime suggests that this may be precisely

⁷⁷NIICPA, *supra* note 6, §§ 1204(a).

⁷⁸*See* 17 U.S.C. § 506(a) (1994); 18 U.S.C.A. § 2319 (West, WESTLAW through P.L. 104-333, approved Nov. 12, 1996).

⁷⁹One of the first discussions of CMS to appear in the popular media was Pamela Samuelson, *The Copyright Grab*, *Wired*, Jan. 1996, at 134, 188-89.

⁸⁰*See, e.g.,* Stefik, *Shifting the Possible*, *supra* note 2; IFRRO Report, *supra* note 2.

⁸¹NIICPA, *supra* note 6, §§1201-1202.

the result its drafters had in mind.) The significance of that interpretation for the reading, viewing, and listening public bears closer examination.

Thus far, much of the debate over the validity of contractual restrictions on the use of copyrighted works has focused on the voluntariness, or lack thereof, of so-called "shrinkwrap" licenses.⁸² Until recently, that question, although important, had largely distracted courts and commentators from the more fundamental, and far more difficult, question of copyright preemption.⁸³ Two recent high-profile cases and a number of thoughtful articles suggest that the issue of copyright preemption may be moving to the forefront.⁸⁴ Representatives of various copyright-related industries are now working to reshape the law of contract voluntariness, via a new Article 2B for the Uniform Commercial Code, in a way that validates shrinkwrap or "click-through" licenses.⁸⁵ Section 2B-319 of the most recent draft effectively validates CMS; it

⁸²See, e.g., David A. Einhorn, *Box-Top Licenses and the Battle-of-the-Forms*, 5 Software L.J. 401 (1992); Robert W. Gomulkiewicz & Mary L. Williamson, *A Brief Defense of Mass Market Software License Agreements*, 22 Rutgers Computer & Tech. L.J. 335 (1996); Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. Cal. L. Rev. 1239 (1995) [hereinafter Lemley, *Shrinkwrap Licenses*]; Mark A. Lemley, *Shrinkwraps in Cyberspace*, 35 Jurimetrics J. 311 (1995); Gary H. Moore & J. David Hadden, *On Line Software Distribution: New Life for 'Shrinkwrap' Licenses?*, Computer Law., Apr. 1996, at 1; Michael Rustad & Lori E. Eisenschmidt, *The Commercial Law of Internet Security*, 10 High Tech. L.J. 213, 290-93 (1995); Michael G. Ryan, *Offers Users Can't Refuse: Shrink-Wrap License Agreements as Enforceable Adhesion Contracts*, 10 Cardozo L. Rev. 2105 (1989); Richard H. Stern, *Shrink-Wrap Licenses of Mass Marketed Software: Enforceable Contracts or Whistling in the Dark?*, 11 Rutgers Computer & Tech. L.J. 51, 55 (1985).

⁸³But see David A. Rice, *Public Goods, Private Contract, and Public Policy: Federal Preemption of Software License Prohibitions Against Reverse Engineering*, 53 U. Pitt. L. Rev. 543 (1992) (providing exhaustive analysis of the copyright preemption issue).

⁸⁴See *National Basketball Association v. Motorola, Inc.*, 105 F.3d 841, 848-53 (2d Cir. 1997) (upholding defense of copyright preemption of state law misappropriation claim); *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1454-55 (7th Cir. 1996) (rejecting defense of copyright preemption of state law breach of contract claim); I. Trotter Hardy, *Contracts, Copyright and Preemption in a Digital World*, 1 Rich. J.L. & Tech. 2 (April 11, 1995) <<http://www.urich.edu/~jolt/v1i1/hardy.html>>; Lemley, *Shrinkwrap Licenses*, *supra* note 82, at 1255-59, 1266-74; Maureen A. O'Rourke, *Drawing the Boundary Between Copyright and Contract: Copyright Preemption of Software License Terms*, 45 Duke L.J. 479 (1995); Elkin-Koren, *supra* note 72.

⁸⁵See U.C.C. Art. 2B: Licenses § 2B-308 (Proposed Draft March 21, 1997), available from the National Conference of Commissioners on Uniform State Laws (visited April 18, 1997) <<http://www.law.upenn.edu/library/ulc/ucc2/ucc2b397.htm>> [hereinafter Draft Article 2B]; Dan

expressly allows use of "a program, code or an electronic or other device that restricts use" of digital information to "prevent[] use of the information in a manner inconsistent with the license."⁸⁶ Yet even assuming a click-through digital license that is (or has been defined to be) entirely voluntary, the question remains whether the restrictions that the license seeks to impose are legitimate.

If digital copyright management systems become widespread, the courts and Congress will need to confront the preemption issue. Here are some factors that should be considered.

First, although the Copyright Act does not preempt state contract law, it may preempt particular contract terms that have the effect of creating rights equivalent to those afforded under copyright law.⁸⁷ The rationale for finding that a contract does not have this effect--employed most recently by the Seventh Circuit in *ProCD, Inc. v. Zeidenberg*,⁸⁸--is that any contract binds only its parties, and thus cannot establish rights against the world.⁸⁹ Assuming the truth of this reasoning, it is not at all clear that it applies to mass-market "licenses" establishing universal conditions of access. Excluding mass-marketed software, the typical copyright license agreement imposes restrictive terms on a small population of customers to prevent the loss of trade-secret information. The license establishes a confidential relationship between the copyright owner and its customers, who otherwise would be free to reverse engineer the product and/or to sell or give

Goodin, *Seeking New Rules for a New Game: Commercial Code Meets the Digital Age*, *Legal Times*, Nov. 4, 1996, at 2; Raymond T. Nimmer, *UCC Revision: Information Age in Contracts*, in American Law Institute--American Bar Association Continuing Legal Education, ALI-ABA Course of Study: The Emerged and Emerging New Uniform Commercial Code 17 (Dec. 12, 1996).

⁸⁶Draft Article 2B, *supra* note 85, § 2B-314(a)(4); *see also id.* § 2B-314(a)(1)-(3) (allowing automatic termination of use of the licensed information upon expiration of the license term if the license so provides, if the electronic system provides "reasonable notice," or if the information is licensed for short-term use).

⁸⁷*See* 17 U.S.C. § 301(a) (1994); H.R. Rep. 94-1476, at 132 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5748 (stating no intent to preempt state contract law generally); *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1455 (7th Cir. 1996) (declining to find preemption of challenged contract term but declining to hold that any contract term escapes preemption as a matter of law); *National Car Rental Sys., Inc. v. Computer Assocs. Int'l*, 991 F.2d 426, 431-35 (8th Cir. 1993) (same); Lemley, *Shrinkwrap Licenses*, *supra* note 82, at 1257-58, 1259-72; O'Rourke, *supra* note 84, at 518-55; Rice, *supra* note 83, at 604-21.

⁸⁸86 F.3d 1447 (7th Cir. 1996).

⁸⁹*Id.* at 1454.

away their individual copies.⁹⁰ The argument that the copyright owner of a mass-marketed work can create a confidential relationship with the entire world is, quite simply, ridiculous. A restriction applied to the entire public amounts to private legislation.⁹¹ At the very least, such a "license" should be subjected to a preemption analysis entirely different from that applicable to negotiated, non-mass-market contracts.

Second, even if standard-form, "click-through" licenses for access to intellectual property are pronounced voluntary and enforceable, the voluntariness inquiry should not stop there. Conventional wisdom is that such licenses preserve consumers' ability to affect vendors' terms and conditions by "voting with their feet" and purchasing from competitors whose terms are more favorable.⁹² CMS should cause us to rethink neoclassical assumptions about market responsiveness to consumer likes and dislikes. They are inexorable, technologically enforced gateways that can be imposed unilaterally, whether consumers like them or not.⁹³ In addition, the number of consumers with strong incentives to object to the new CMS regimes may be small.

⁹⁰See Rice, *supra* note 83, at 622-26 ("It is at least reasonable to argue that reverse engineering is, in most instances, necessarily precluded under a negotiated agreement not to disclose or use trade secret information except as required for computer program installation, adaptation, maintenance or use.").

⁹¹See Robert P. Merges, *Intellectual Property and the Costs of Commercial Exchange: A Review Essay*, 93 Mich. L. Rev. 1570, 1611-13 (1995) (citing Friedrich Kessler, *Contracts of Adhesion--Some Thoughts About Freedom of Contract*, 43 Colum. L. Rev. 629, 640 (1943)) (discussing power disparities surrounding use of standard-form contracts to augment intellectual property rights); Rice, *supra* note 83, at 595 (applying "private legislation" analysis to restrictive software license terms); Cohen, *Right to Read Anonymously*, *supra* note 76, at 1001-02 (applying "private legislation" analysis to CMS); *cf.* O'Rourke, *supra* note 84, at 541-55 (arguing that, generally speaking, even mass-market licenses restricting decompilation should survive preemption analysis, but recognizing exception when copyright owner "has obtained near monopoly power in the relevant market," as measured by antitrust analysis).

⁹²This reasoning is implicit in the Seventh Circuit's decision in ProCD. See 86 F.3d at 1455 (observing that ProCD's license terms would not bar other vendors from compiling and offering the same material); *see also*, e.g., I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U. Pitt. L. Rev. 993, 1019-21, 1028-36 (1994).

⁹³*Cf.* Lawrence Lessig, *The Zones of Cyberspace*, 48 Stan. L. Rev. 1403, 1408 (1996) ("Code is an efficient means of regulation. . . . One obeys these laws as code not because one should; one obeys these laws as code because one can do nothing else. . . . In the well implemented system, there is no civil disobedience."); Edward L. Rubin, *The Nonjudicial Life of Contract: Beyond the Shadow of the Law*, 90 Nw. U.L. Rev. 107, 125-31 (arguing that repeat players in the contracting process enjoy "simply overwhelming" advantages in implementing the self-help strategies of their choice).

Most simply want to read, listen, and view, not to reverse engineer or parody, and most will be able to afford the fractional fees levied under a "usage rights" regime. And to the extent that copyrighted works are not fungible--i.e., to the extent that consumers want Nimmer on Copyright rather than the copyright summary prepared by a local law firm, or Toni Morrison rather than John Grisham, or Pearl Jam rather than the Cranberries--many consumers may be reluctant to take their business elsewhere.

Finally, if copyright owners prove determined to implement CMS that comprehensively augment the rights afforded them under the Copyright Act, perhaps Congress should consider whether these individuals and entities should be required to elect only contract remedies, and to abandon their claims to copyright protection.⁹⁴ After all, copyright was created to correct market failures arising from the public good characteristic of original expression. If CMS provide a more reliable method of correcting market failure, who needs copyright? I hope that most readers will think this suggestion absurd--and will react that way because they recognize that the semi-permeable barrier of copyright promotes the public interest.⁹⁵ But if the copyright system is

⁹⁴See Tom W. Bell, *Fair Use vs. Fared Use: the Impact of Automated Rights Management on Copyright's Fair Use Doctrine*, 75 N.C. L. Rev. __ (forthcoming 1997) (visited May 7, 1997) <<http://members.aol.com/tombell/FullFared.html>>; Lemley, *Shrinkwrap Licenses*, *supra* note 82, at 1273-74; 1 Melville Nimmer & David Nimmer, *Nimmer on Copyright* § 1.01[B], at 1-16.1 (discussing judicially imposed election of remedies as alternative to holding contract term preempted).

⁹⁵Trotter Hardy argues that in light of the low costs of protecting and transacting in digital content, the current copyright paradigm is an inefficient method of protecting property entitlements and should be replaced with a pure private property rights regime. Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U. Chi. Legal Forum 217, 236-52 (1996). He maintains that conceiving the public law of copyright to represent a variety of stakeholders (including the public) creates a form of group ownership, the inefficiency of which manifests itself in the lengthy, costly legislative process. *See id.* at 253-58. This analysis misses the point for two reasons. First, Congress "assumes" that copyright has multiple stakeholders because the Constitution requires it. *See Feist Publications, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 349-50 (1991) ("[C]opyright assures authors the right to their original expression, but encourages others to build freely upon the ideas and information conveyed by a work."); *Harper & Row, Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 555-60 (1985) ("First Amendment protections . . . [are] embodied in the Copyright Act's distinctions between copyrightable expression and uncopyrightable facts and ideas, and in the latitude for scholarship and comment traditionally afforded by fair use.").

Second, and more fundamental, Hardy's analysis follows only if one assumes that the "point" of copyright is to provide maximum incentives to information creators and thus, necessarily, maximum protection for property entitlements. *See Hardy, supra*, at 220-23 (assuming just this, and discarding from his "taxonomy of incentives" those that do not fit within this model). Nowhere does Hardy acknowledge, much less justify, these assumptions. I (and

necessary, then allowing unlimited numbers of copyright owners to opt out of the system as it suits them is bad law and bad policy. At the very least, a CMS regime should be subject to an analogous set of restrictions designed to balance the affected interests.⁹⁶

B. Reader Privacy and Anonymity

Leading recent surveys of developments in the field of "rights management" describe the capabilities of an ideal system as follows:

"detecting, preventing, and counting a wide range of operations, including open, print, export, copying, modifying, excerpting, and so on;"⁹⁷

maintaining "records indicating which permissions ha[ve] actually been granted and to whom;"⁹⁸

many others) would argue for a more generous conception of copyright's purpose, and would contend that a maximum-incentives regime is not--and certainly has not been proven to be--the best-suited to advancing the ultimate goals that copyright seeks to further. *See, e.g.*, Feist, 499 U.S. at 349 ("The primary objective of copyright is not to reward the labor of authors, but '[t]o promote the Progress of Science and useful Arts.'" (quoting U.S. Const. Art. I, § 8, cl. 8)); Cohen, *Reverse Engineering*, *supra* note 46, at 1104-24 (arguing that the purpose of copyright is not merely to disseminate works to the public as consumers, but to foster access to works by the public as creators, and that a maximum-protection regime does not serve this purpose); Robert A. Kreiss, *Accessibility and Commercialization in Copyright Theory*, 43 UCLA L. Rev. 1 (1995) (same); Jessica Litman, *The Public Domain*, 39 Emory L.J. 965 (1990) (same); Neil Weinstock Netanel, *Copyright and a Democratic Civil Society*, 106 Yale L.J. 283 (1996) (arguing that a purpose of copyright is to promote the deliberation and debate constitutive of a robust democratic public sphere, and that a maximum-protection regime does not serve this purpose); Niva Elkin-Koren, *Cyberlaw and Social Change: A Democratic Approach to Copyright Law in Cyberspace*, 14 Cardozo Arts & Ent. L.J. 215 (1996) (same).

⁹⁶Mark Stefik appears to agree. *See Stefik, Shifting the Possible, supra* note 2, at 156 (recognizing that CMS implicate social policy and advocating the creation of a Digital Property Trust, governed by representatives from all of the affected constituencies, to guide the development of CMS).

⁹⁷IFRRO Report, *supra* note 2, § 3.1.1; *see also* Burns, *supra* note 1, at 17-21, 31-35 (1995); Stefik, *Letting Loose the Light, supra* note 1, at 228-38; Stefik, *Shifting the Possible, supra* note 2, at 140-41.

⁹⁸IFRRO Report, *supra* note 2, § 3.2.

"captur[ing] a record of what the user actually looked at, copied or printed;"⁹⁹ and sending "this usage record . . . to the clearinghouse when the user seeks additional access, at the end of a billing period or whenever the user runs out of credit."¹⁰⁰

In addition, the system operator could manipulate this acquired data to generate predictive profiles of particular consumers for use in future marketing activities, or for sale to other vendors.¹⁰¹ These capabilities, if realized, threaten individual privacy to an unprecedented degree. Although credit-reporting agencies and credit card providers capture various facets of one's commercial life, CMS raise the possibility that someone might capture a fairly complete picture of one's intellectual life.

Reading, listening, and viewing habits reveal an enormous amount about individual opinions, beliefs, and tastes, and may also reveal an individual's association with particular causes and organizations. Equally important, reading, listening, and viewing contribute to an ongoing process of intellectual evolution. Individuals do not arrive in the world with their beliefs and opinions fully-formed; rather, beliefs and opinions are formed and modified over time, through exposure to information and other external stimuli.¹⁰² Thus, technologies that monitor

⁹⁹Burns, *supra* note 1, at 32; *see also* Mary G. Smith & Robert Weber, *A New Set of Rules for Information Commerce--Rights-Protection Technologies and Personalized-Information Commerce Will Affect All Knowledge Workers*, *Comm. Week*, Nov. 6, 1995, at 34, 36-37.

¹⁰⁰Burns, *supra* note 1, at 32; *see also* Stefik, *Letting Loose the Light*, *supra* note 1, at 241 (describing the creation of transaction repositories and electronic clearinghouses to process CMS charges).

¹⁰¹*See* Cohen, *Right to Read Anonymously*, *supra* note 76, at 985-86; Froomkin, *supra* note 45, at 484-88; Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights*, 44 *Fed. Comm. L.J.* 195, 200-06 (1992); Debra Aho Williamson, *Smart Agents Build Brains Into Net Ads: More Companies Tap Technology to Better Target Web Users Who Visit Their Sites*, *Advertising Age*, Apr. 8, 1996, at 26. For an example of an existing Internet-based content vendor that conducts "push" marketing based on customized consumer profiles unless the consumer expressly "opts out" of this activity, see the World Wide Web site of CDNow, <<http://cdnow.com/>>; *see also* Donna Hoffman, et al., *Social Issues Raised by the Commercial Development of the Net*, *Panel Presentation at The Seventh Conference on Computers, Freedom and Privacy* (March 12, 1997) (presentation by Jason Olim, President of CDNow).

¹⁰²*See* Cohen, *Right to Read Anonymously*, *supra* note 76, at 1006-07; Niva Elkin-Koren, *Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of Bulletin Board Operators*, 13 *Cardozo Arts & Ent. L.J.* 346, 400 (1995); *cf.* Netanel, *supra* note 95, at 347-62 (arguing that the widespread dissemination of works of

reading, listening, and viewing habits represent a giant leap--whether forward or backward the reader may decide--toward monitoring human thought. The closest analogue, the library check-out record, is primitive by comparison. (And library check-out records are subject to stringent privacy laws in most states.¹⁰³

I have argued elsewhere that the freedom to read, listen, and view selected materials anonymously should be considered a right protected by the First Amendment, and that if it is so protected, the NIICPA's civil and criminal penalty provisions are vulnerable to constitutional challenge.¹⁰⁴ I will not revisit that argument here. Whether or not the NIICPA presents a First Amendment question, its privacy implications are clear and disturbing.

Designing CMS that are less invasive than the "ideal" technologies described above is of course possible. For example, a system might simply prohibit access or copying/printing without some initial payment, or incorporate serial-copy-management technology similar to that required under the Audio Home Recording Act.¹⁰⁵ It might preserve privacy by preventing the extraction of personal identifying data or accepting payments in anonymous "digital cash."¹⁰⁶ For the most part, however, at least in this country, those involved in the development of CMS appear

authorship facilitated by copyright creates and enhances deliberation and debate among citizens).

¹⁰³See, e.g., Alaska Stat. § 09.25.140 (1994); Cal. Gov't Code § 6254(j) (West 1995); Del. Code Ann. tit. 29, § 10002(12) (1991); Ill. Ann. Stat. ch. 81, para. 1201 (Smith-Hurd 1993); N.Y. Civ. Prac. Law § 4509 (McKinney 1992). See also Cohen, *Right to Read Anonymously*, *supra* note 76, at 1031-32 n.213 (listing state legislation passed to protect the identities of library patrons).

¹⁰⁴Cohen, *Right to Read Anonymously*, *supra* note 76, at 1003-30.

¹⁰⁵17 U.S.C. § 1002(c) (1994).

¹⁰⁶See Fromkin, *supra* note 45, at 415-20, 459-70 (discussing anonymous-payer digital cash); Smith & Weber, *supra* note 99, at 36 ("To protect the privacy of individuals . . . the usage data can be aggregated or made anonymous before it reaches rights holders."); cf. Dorothy J. Glancy, *Privacy and Intelligent Transportation Technology*, 11 Santa Clara Computer & High Tech. L.J. 151, 181-83 (1995) (observing that the most effective way to protect individual privacy in the digital age is to design technological tools so that they prevent or limit the identification of individuals); Jeffrey H. Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 Santa Clara Computer & High Tech. L.J. 27, 43-44 (1995) (suggesting that "physical realities that hinder others in gathering information about or experiences of you" provide more effective protection than privacy laws that attempt to compensate for the ease of information gathering).

enthusiastic about the prospect of generating individual usage records, and relatively unconcerned with reader privacy.¹⁰⁷

After enough time and consumer outcry, the copyright management industry will likely decide to regulate its own privacy practices in some fashion.¹⁰⁸ The Information Infrastructure Task Force's Working Group on Privacy Rights recommended a series of principles to serve as the basis for voluntary, private-sector privacy policies, and the National Telecommunications and Information Administration has followed up with a more concrete proposal based on principles of informed consent.¹⁰⁹ This disclosure-based proposal, however, falls well short of vesting readers with an entitlement to prevent the collection of personal information and to control the uses to which it is put. And, as noted above, there is reason to doubt that information consumers will be able to effect substantial changes in the structure of private CMS regimes. Accordingly, legislation seems a more reliable way of guaranteeing a baseline level of reader privacy that is acceptable to consumers.

Although many other nations and the European Union have enacted general-purpose privacy laws, the United States has not done so.¹¹⁰ Instead, it has relied on narrow context-specific

¹⁰⁷See, e.g., Burns, *supra* note 1, at 36 (characterizing privacy concerns as "market acceptance problems"). *But see* Proceedings of the First IMPRIMATUR Consensus Forum 86-90 (1996), (visited April 18, 1997) <<http://www.imprimatur.alcs.co.uk/html/page15.htm>> (concluding that the European IMPRIMATUR project to develop a standardized model for CMS should recognize reader privacy as a fundamental right and build "Privacy-Enhancing Technologies" into the CMS model).

¹⁰⁸Recent presentations at the 1997 Conference on Computers, Freedom, and Privacy indicate that self-policing initiatives are underway, motivated at least in part by a desire to avoid government regulation. The most promising of these initiatives appears to be ETrust, an effort to create a taxonomy of privacy policies and rating symbols that convey information on privacy practices to consumers. For information on ETrust, see the organization's World Wide Web site at <<http://www.etrust.org/>>.

¹⁰⁹See U.S. Dep't of Commerce, Information Infrastructure Task Force, Privacy Working Group, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information (1995), (visited April 18, 1997) <http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html>; U.S. Dep't of Commerce, National Telecommunications and Information Administration, Privacy and the NII: Safeguarding Telecommunications-Related Personal Information (1995) (visited Apr. 18, 1997) <<http://www.ntia.doc.gov/ntiahome/privwhitepaper.html>>.

¹¹⁰See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31; Dennis Campbell & Joy Fisher, eds., Data

legislation, such as the "Bork bill" concerning privacy of video rental records, to address perceived threats to privacy.¹¹¹ The most recent example of such legislation is the recently introduced Consumer Internet Privacy Protection Act of 1997, which is intended to impose restrictions on the use of personal identifying data collected by an "interactive computer service."¹¹² Although this language arguably is broad enough to cover operators of on-line CMS, the definition of "interactive computer service" suggests that the bill is intended to apply only to on-line service providers.¹¹³ If that is the case, then there is no current or pending legislation that might serve to safeguard reader privacy in cyberspace.

Elsewhere, I have suggested the form that reader privacy legislation should take and some of the elements it should contain.¹¹⁴ Here, I wish only to argue that some Congressional response to the privacy threat posed by CMS is necessary. This is so whether or not Congress adopts implementing legislation to protect CMS against unlawful tampering. If, as seems overwhelmingly likely, some anti-tampering legislation is enacted, Congress should consider the possibility that individuals might wish to tamper with CMS to preserve their privacy, and should make an express, considered decision whether and to what extent the provisions of an anti-tampering law should apply to such conduct.

V. Conclusion

I do not intend to suggest that CMS should receive no protection whatsoever. As this article makes evident, however, both CMS and laws designed to protect them warrant far closer public scrutiny than they have been given. Also evident from the vigorous opposition to the NIICPA, and to the United States' proposals for the WIPO copyright treaty, is that many disagree with the Clinton Administration regarding the scope of protection that is necessary and desirable. The upcoming treaty ratification and implementation process should include careful consideration of the implications of CMS, so that the public understands the exact bargain it is making in enacting laws for their protection.

Transmission and Privacy (1994) (surveying status of privacy protection in 19 European, Asian, and North American countries).

¹¹¹18 U.S.C.A. § 2710 (West, WESTLAW through P.L. 104-333, approved Nov. 12, 1996); *see* Reidenberg, *supra* note 101 (outlining and critiquing the piecemeal privacy protection available against private-sector collection, use, and sale of personal information); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 Iowa L. Rev. 497 (1996) (same).

¹¹²Consumer Internet Privacy Protection Act of 1997, H.R. 98, 105th Cong. § 2 (1997).

¹¹³*Id.* § 4(1).

¹¹⁴Cohen, *Right to Read Anonymously*, *supra* note 76, at 1031-38.