1996

# A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace

Julie E. Cohen
*Georgetown University Law Center*, jec@law.georgetown.edu



28 Conn. L. Rev. 981-1039 (1996)

# A RIGHT TO READ ANONYMOUSLY: A CLOSER LOOK AT "COPYRIGHT MANAGEMENT" IN CYBERSPACE

**Julie E. Cohen***

**Originally published 28 Conn. L. Rev. 981 (1996).**

It has become commonplace to say that we have entered the age of information. The words conjure up images of a reader's paradise — an era of limitless access to information resources and unlimited interpersonal communication. In truth, however, the new information age is turning out to be as much an age of information *about* readers as an age of information *for* readers. The same technologies that have made vast amounts of information accessible in digital form are enabling information providers to amass an unprecedented wealth of data about who their customers are and what they like to read. In the new age of digitally transmitted information, the simple, formerly anonymous acts of reading, listening, and viewing — scanning an advertisement or a short news item, browsing through an online novel or a collection of video clips — can be made to speak volumes, including, quite possibly, information that the reader would prefer not to share.

This Article focuses specifically on digital monitoring of individual reading habits for purposes of so-called "copyright management" in cyberspace, and evaluates the import of this monitoring for traditional notions of freedom of thought and expression.[1] A fundamental

---

*Assistant Professor, University of Pittsburgh School of Law. J.D., Harvard Law School, 1991. I thank Tom Bell, Martha Chamallas, Ruth Colker, Susan Freiwald, Michael Froomkin, Arthur Hellman, Bernard Hibbitts, Mark Lemley, Jessica Litman, Pamela Samuelson, and Lee Tien for helpful comments on earlier drafts, and Jim Williams and Mauri Aven for their able research assistance.

[1]Much has been written about the impact of new digital technologies on individual privacy generally. *See, e.g.*, Anne Wells Branscomb, Who Owns Information? From Privacy to

assumption underlying our discourse about the activities of reading, thinking, and speech is that individuals in our society are guaranteed the freedom to form their thoughts and opinions in privacy, free from intrusive oversight by governmental or private entities. The new copyright management technologies force us to examine anew the sources and extent of that freedom.

Part I of this Article describes the various copyright management technologies that are being developed to enable copyright owners to monitor readers' activities in cyberspace and the uses they make of reading materials acquired there. Part II provides an overview of proposed federal legislation designed to reinforce copyright owners' power unilaterally to institute intrusive copyright management systems. Part III considers, and rejects, the possibility that the impending digital copyright management regime constitutes no more than legitimate private ordering regarding the terms and conditions of access to copyrighted works. Part IV discusses the sources and justifications for an individual right to read anonymously, and argues that reading

---

Public Access (1994); Oscar H. Gandy, Jr., The Panoptic Sort: A Political Economy of Personal Information (1993); Anne Wells Branscomb, *Internet Babylon? Does the Carnegie Mellon Study of Pornography on the Information Superhighway Reveal a Threat to the Stability of Society?*, 83 GEO. L.J. 1935 (1995); Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 601 (1996); A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395 (1996); Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights*, 44 FED. COMM. L.J. 195 (1992); Joe R. Reidenberg & Francoise Gamet-Pol, *The Fundamental Roel of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105 (1995); Glenn C. Smith, *We've Got Your Number! (Is It Constitutional to Give It Out?): Caller Identification Technology and the Right to Informational Privacy*, 37 UCLA L. REV. 145 (1989); Symposium, *Privacy and IVHS*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 13 (1995); Symposium, *Data Protection Law and the European Union's Directive: The Challenge for the United States*, 80 IOWA L. REV. 431 (1995); *see also* Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 3-11 (1991) (predicting that the modern "information explosion" will exacerbate existing tensions in constitutional privacy doctrine). This Article will not revisit that ground, but will focus more specifically on the relationship between privacy, anonymity, and freedom of thought and expression. As used in this Article, "reading" includes viewing and listening.

is so intimately connected with speech and freedom of thought that the First Amendment should be understood to guarantee such a right. Part V suggests that proposed federal protection for digital copyright management technologies may be unconstitutional to the extent that it penalizes individuals who seek only to exercise their rights to read anonymously, or to enable others to do so. Finally, Part VI argues that rather than seeking to enshrine a set of practices designed to negate reader anonymity, Congress should, instead, adopt comprehensive legislation designed to shield individual reading habits from scrutiny.

## I. THE NEW COPYRIGHT MANAGEMENT TECHNOLOGIES

The amount of copyrighted material available online has grown exponentially in the last few years, and will continue to do so for the foreseeable future.[2] The same technologies that enable readers to access digitally stored works, however, also enable copyright owners to generate precise and detailed records of such access. Copyright owners then can use that data, together with other new technological tools, to monitor on a continuing basis, and extract additional royalties for, readers' subsequent uses of the works they have acquired.[3] Thus, for

---

[2]*See, e.g.*, *Economic Indicators*, THE ECONOMIST, Feb. 24, 1996, at 110 (number of Internet hosts growing at 85% annually, and number of multi-media World Wide Web pages growing at 2500% annually).

[3]Consistent with the planned extraction of royalties on a per-use basis, copyright owners and developers of copyright management systems refer to the initial transaction in the copyrighted work as a "license" rather than a sale. Whether purveyors of copyrighted works held out for mass-market purchase may characterize consumer transactions as licenses to justify imposing more restrictive terms than allowed by copyright law is hotly debated, as is the larger question whether copyright law and the substantive policies it embodies preempt certain contract terms outright. *See, e.g.* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1453-55 (concluding that contract terms ordinarily will not be preempted) (7th Cir. 1996); Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239 (1995); 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). The proposed Article 2B of the Uniform Commercial Code, which is intended to cover licensing of intangibles, makes no reference to this these debates. *See* Draft Revised Article 2B: Licenses, *available*

example, if I purchase a collection of essays online, the copyright owner can charge me for the file containing the essays, generate a record of my identity and what I purchased, and insert pieces of microcode into the file that will: (1) notify the copyright owner every time I "open" one of the essays and specify which one I opened; (2) notify me when I must remit additional fees to the copyright owner — this much to browse the essay, this much to print it out, this much to extract an excerpt, and so on; and (3) prevent me from opening, printing, or excerpting the piece until I have paid. Together, these new digital monitoring and metering technologies define the burgeoning field of "copyright management."[4] Within the last two years, a copyright management industry has begun to emerge, directed at the development of integrated systems that can not only conduct online transactions and generate customer records, but also implement desired technological and pricing restrictions on subsequent uses of copyrighted works.[5]

---

*online* <http://www.lawlib.uh.edu/ucc2b/0503/0503_2b.html.> This Article will not address the question of copyright preemption of license terms, except to note that the answer will affect significantly the range of copyright management practices a copyright owner may lawfully adopt. *See infra* notes 42-43 and accompanying text.

[4]*See* Mary Grace 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; Mark Stefik, *Letting Loose the Light: Igniting Commerce in Electronic Publication*, in MARK STEFIK, ED., INTERNET DREAMS: ARCHETYPES, MYTHS, AND METAPHORS 3 (forthcoming MIT Press 1996); Robert Weber, *Digital Rights Management Technologies*, *available online* <http://www.ncri.com/articles/rights_management/> (describing desired functions and capabilities of a copyright management system and surveying available technologies and providers).

[5]*See* CHRISTOPHER BURNS, COPYRIGHT MANAGEMENT AND THE NII: REPORT TO THE ENABLING TECHNOLOGIES COMMITTEE OF THE ASSOCIATION OF AMERICAN PUBLISHERS (1995); Charles Clark, *The Publisher in the Digital World*, *in* INTELLECTUAL PROPERTY RIGHTS AND NEW TECHNOLOGIES: PROCEEDINGS OF THE KNOWRIGHT '95 CONFERENCE 85, 96-101 (1995); Smith & Weber, *supra* note 4; Stefik, *supra* note 4; Mark Stefik, *Shifting the Possible: How Digital Property Rights Challenge Us To Rethink Digital Publishing* (1996) (unpublished paper on file with author); Steve G. Steinberg, *Software Metering*, WIRED 3.07, July 1995, at 137; Steve G. Steinberg, *Tracking Usage Rights*, WIRED 3.07, July 1995, at 140; Steve G. Steinberg, *Digital Watermarks*, WIRED 3.07, July 1995, at 141; Weber, *supra* note 4; *see also* John Perry

As justification for the development of digital copyright management systems, copyright owners cite the ease of reproducing and transmitting unauthorized copies of digital works over electronic networks. They argue that technological protection for their works is necessary to prevent widespread infringement, thus giving them the incentive to make their works available online.[6] As the above example suggests, however, many copyright owners envision copyright management systems that will be capable of doing far more than simply preventing unauthorized reproduction. One study of existing technologies for copyright management characterizes the ideal technology as "capable of detecting, preventing, and counting a wide range of operations, including open, print, export, copying, modifying, excerpting, and so on."[7] In addition, the wish

---

Barlow, *The Economy of Ideas: A Framework for Rethinking Patents and Copyrights in the Digital Age*, WIRED 2.03 March 1994, at 84, 129; Esther Dyson, *Intellectual Value*, WIRED 3.07, July 1995, at 136, 139, 184.

[6]*See, e.g.*, *On-Line Security Issues: Hearings on S. 1726 Before the Subcomm. on Science, Technology and Space of the Senate Comm. on Commerce*, 104th Cong., 2d Sess. (June 12, 1996) (statement of Jack Valenti, Chairman and Chief Executive Officer, Motion Picture Association of America, Inc.), *available online* WESTLAW, USTestimony database; *National Information Infrastructure: Hearings on S 1284 Before the Senate Comm. on the Judiciary*, 104th Cong., 2d Sess. (May 7, 1996) (statement of Kenneth R. Kay, Executive Director, Creative Incentive Coalition), *available online* 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., 2d Sess. (Feb. 7, 1996) (statements of the Association of American Publishers; Barbara A. Munder, Senior Vice President, The McGraw-Hill Companies; Frances W. Preston, President and CEO, Broadcast Music, Inc.; Jack Valenti, Chairman and Chief Executive Officer, Motion Picture Association of America, Inc.), *available online* WESTLAW, USTestimony database; Creative Incentive Coalition, *Ten Myths About the NII Copyright Protection Act* (1996), *available online* http:/www.cic.org/myths.html; *see also* U.S. DEP'T OF COMMERCE, INFORMATION INFRASTRUCTURE TASK FORCE, WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS, 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].

[7]Weber, *supra* note 4, § 3.1.1; *see also* BURNS, *supra* note 5, at 17-21, 31-35; Clark, *supra* note 5, at 97-99; Stefik, *supra* note 4, at 14-24; Steinberg, *Software Metering*, *supra* note 5; Steinberg, *Usage Rights*, *supra* note 5.

list continues, the copyright management system should maintain "records indicating which permissions ha[ve] actually been granted and to whom."[8] The system can then create a record each time the work is used and notify the copyright owner if additional "usage rights" are sought.[9] This vision of the future of copyright management could entail total loss of reader anonymity in cyberspace.[10]

In addition to using new digital technologies to exert continuing control over readers' uses of digital works, some copyright owners may use the transaction records generated by their copyright management systems to learn more about their customers through a process known as "profiling." The activity of profiling, per se, is not new. It is a well-established practice through which businesses of all types seek to learn as much as possible about customers who show interest in their products or services. For transactions that occur in "real" (as opposed to digital) space, however, the ability to profile one's customer base is limited to some extent by customers' willingness to self-report — for example, by filling out product registration cards. In contrast, profiling in the digital age holds out, for the first time, the tantalizing promise of "perfect" information, because digital communications can be structured to create detailed records of consumer purchases and reading activities.[11]

---

[8]Weber, *supra* note 4, § 3.2.

[9]*See, e.g.*, BURNS, *supra* note 5, at 32 ("In addition to regulating access to the local database, the systems capture a record of what the user actually looked at, copied or printed, and this usage record is sent to the clearinghouse when the user seeks additional access, at the end of a billing period or whenever the user runs out of credit."); Smith & Weber, *supra* note 4, at 36-37.

[10]It could also entail the demise of the fair use doctrine. *See* Pamela Samuelson, *The Copyright Grab*, WIRED 4.01, Jan. 1996, at 134. However, that is a subject for another article.

[11]*See* Alan Wexelblat, *How Is the NII Like A Prison?*, *available online* <http://wex.www.media.mit.edu/people/wex/panoptic-paper.html> (characterizing profilers' goal

At its most crude, profiling might consist of gathering basic demographic information about readers who "visit" a copyright owner's site on the World Wide Web and/or acquire digital copies of copyrighted works made available there. When I pay for the collection of essays, my electronic mail address and, if applicable, credit card information, furnish some information about my identity.[12] More sophisticated reader profiling is made possible by the use of intelligent "search agents" that comb the World Wide Web for other information about me — other things I have purchased, discussion groups and news groups to which I belong, and so on.[13] The copyright owner may also use complex "data mining" techniques that analyze its customer database, together with personal data purchased or acquired from other sources, to identify patterns or correlations that might illuminate the preferences of particular types of customers.[14]

---

as "the panoptic sort," an "information collection and use regime" that will enable perfect prediction of individual conduct); *see generally* GANDY, *supra* note 1. In cyberspace, of course, "perfect" information is a myth. Email addresses may be shared by families or even by co-workers, so that it may be impossible to assemble accurate demographic profiles. However, that is unlikely to deter digital profilers from trying.

[12]*See, e.g.*, Mitch Betts, *Privacy Fades for Web Visitors: Lust for Data, New Tracking Techniques Dog Users*, COMPUTERWORLD, Sept. 25, 1995, at 162; Steve Moore, *Internet Security Split: Let the Browser Beware*, COMPUTERWORLD, Aug. 28, 1995, at 59; Froomkin, *supra* note 1, at 484-88. Industry commentators refer to such Web site "hits" as "mouse droppings." *See, e.g.*, Larry Irving, *Progress Report on the Information Superhighway: Privacy High on the Fed's Priority List — Surprised?*, MACWORLD, Mar. 1996, at 260.

[13]*See, e.g.*, Betts, *supra* note 12 (describing "DejaNews" search tool that allows retrieval of individuals' postings to Usenet discussion groups); Forbes ASAP, *How Smart Agents Will Change Selling*, FORBES, Aug. 28, 1995, at 95; Debra Aho Williamson, *Smart Agents Build Brains Into Net Ads: More Companies Tap Technology to Better Target Web Users Who Visit Their Sites*, ADVERTIZING AGE, Apr. 8, 1996, at 26.

[14]*See* Reidenberg, *supra* note 1, at 200-06 & n.42 ("Random House is testing a database that enables it to send specialized mail order catalogs to customers with specific reading preferences."); Reidenberg & Gamet-Pol, *supra* note 1, at 112, 121-22; Dan Richman, *Data Mining Chisels Its Niche*, COMPUTER WORLD, Jan. 29, 1996, at 49 (explaining general principles of data mining); Froomkin, *supra* note 1, at 481-88 (describing the convergence of sophisticated data mining techniques with the increased availability of data pertaining to individual histories,

The copyright owner can then use the information it has amassed about my tastes and purchasing habits to market other works to me. It can also sell the information to third parties.

None of these intrusions need occur. A digital copyright management system could perform the essential continuing control functions while still preserving reader anonymity. At its most basic, such a system might simply provide pricing information, negotiate the purchase transaction, and release a copy of the work for downloading to the customer's computer — without generating permanent customer records at all. While some consumers might choose to pay for digital works with credit cards, thereby revealing their identities, others might opt for some form of anonymous-payer digital cash.[15] Even for credit card purchases, the copyright owner could design a system that would retain records of user identities only until payment is received and/or that would deny copyright owners the ability to extract the individualized transaction data necessary to conduct reader profiling. Getting slightly more complicated, one could also imagine a remote debit system that would simply extract an additional, but anonymous, payment from the reader each time the work is used in a designated way.[16] Finally, to prevent unauthorized copying, the copyright owner could simply insert a piece of microcode in every copy of a digital work that would automatically bar the reader from making perfect

---

purchasing patterns, and reading habits); U.S. DEP'T OF COMMERCE, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION app. (1995) [hereinafter NTIA PRIVACY REPORT] (same); Wexelblat, *supra* note 11, at 2-4 (same).

[15]*See* Froomkin, *supra* note 1, at 415-20, 459-70.

[16]*See* Smith & Weber, *supra* note 4, at 36 ("To protect the privacy of individuals . . . the usage data can be aggregated or made anonymous before it reaches rights holders.");Weber, *supra* note 4, S2.5.2.1; *cf.* Dorothy J. Glancy, *Privacy and Intelligent Transportation Technology*, 11 SANTA CLARA CPTR. & 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).

second-generation digital copies, or from printing more than one copy.[17] Similar "serial copy management" technology is now required in all digital audio recording devices and media sold in the United States.[18]

It is not yet apparent which model, if any, will become the standard for online copyright management. However, neither private nor public research efforts appear to contemplate built-in technological limits on copyright owners' monitoring capabilities. The Library of Congress, in conjunction with the Corporation for National Research Initiatives and the Department of Defense, is working to develop an automated copyright registration and recordation system that will incorporate a prototype "rights management" component.[19] The publicly-available documentation for the system does not indicate what measures, if any, have been taken to

---

[17]*See, e.g.*, Stefik, *supra* note 4, at 31; Stefik, *supra* note 5, at 4.

[18]*See* 17 U.S.C. §§ 1001-1002. Without the required modifications, digital audio recording devices can produce near-perfect copies of musical recordings. The "serial copy management" provisions were added to the Copyright Act to prevent the development of a market in unauthorized "perfect" second-generation recordings. *See* H.R. REP. NO. 102-873(II), 102d Cong., 2d Sess. 2 (1992), *reprinted in* 1992 U.S.C.C.A.N. 3578, 3601. The provisions were drafted to exclude computers and computer programs from the definitions of "digital audio recording medium" and "digital musical recording." 17 U.S.C. § 1001(4)(B)(ii), (5)(B)(ii); *see* 138 CONG. REC. H9029, H9033 (statement of Rep. William Hughes, then-chairman of the Subcommittee on Intellectual Property of the House Judiciary Committee). An analogous provision for inclusion of serial copy management technology in digital works published in cyberspace easily could be drafted. For a discussion of various anti-copying functions and strategies that might be incorporated into digital copyright management systems, see BURNS, *supra* note 5, at 15-21, 44-47.

[19]NII WHITE PAPER, *supra* note 6, at 192 & n.518. The rights management system is conceived as a means for licensing rights in copyrighted works using electronic mail. *See* Robert E. Kahn, *Deposit, Registration and Recordation in an Electronic Copyright Management System available online* <http://www.nlc-bnc.ca/documents/infopol/copyright/kahn.txt.> Field tests of the system began in late 1994. Otis Port, *Halting Highway Robbery on the Internet*, BUSINESS WEEK, Oct. 17, 1994, at 212.

preserve for would-be readers an option to remain anonymous.[20] Privacy is discussed only with reference to the use of public key cryptography to keep purchase transactions secure from third parties.[21] Private industry groups also are working to develop their own copyright management systems and standards.[22] The Copyright Clearance Center, which handles photocopy licensing for many large copyright owners, is developing a system capable of extremely fine-grained monitoring and control.[23] A number of computer technology companies are pursuing similar capabilities, and the Association of American Publishers is following their progress closely.[24] Concern for reader privacy appears limited to the "market acceptance problems" that might develop once systems to capture "detailed report[s] of daily usage" are in place.[25] Thus, it seems

---

[20]*See* NII WHITE PAPER, *supra* note 6, at 192 & n.518; U.S. Copyright Office, *Copyright Office Electronic Registration, Recordation and Deposit System*, *available online* <http://lcweb.loc.gov/copyright/cords.html.>

[21]*See* Kahn, *supra* note 19. For a brief overview of public key cryptography, see Froomkin, *supra* note 1, at 418-419 & n.74. For more in-depth treatments of cryptography generally and the encryption of digital communications in particular, *see* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 19-56 (1994); A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 713-14, 718-63 (1995).

[22]It is unlikely that the government would mandate adoption of the Copyright Office's system by copyright owners who prefer something different. As in other areas of federal technology policy, it is more likely that future legislation or regulation in this area will simply encourage private sector development of systems and standards. This is the approach recommended by the government in the NII WHITE PAPER. NII WHITE PAPER, *supra* note 6, at 233 ("Copyright owners should be free to determine what level or type of protection (if any) is appropriate for their works, taking into consideration cost and security needs, and different consumer and market preferences.").

[23]*See* Weber, *supra* note 4, §§ 3.3, 5.5.1

[24]See BURNS, *supra* note 5, at 30-35; Weber, *supra* note 4.

[25]Burns, *supra* note 5, at 36; *see also* Reidenberg, *supra* note 1, at 206-07 (noting disparity between industry and individual views on consumer privacy issues).

certain that the digital copyright management systems of the not-so-distant future will enable copyright owners who desire it to maintain comprehensive databases of who is reading what.

The National Telecommunications and Information Administration recently released a report that discusses in some depth the implications of digital monitoring technologies and profiling practices for individual privacy.[26] However, no statutory or regulatory barrier currently exists that would preserve a right of anonymity for readers who purchase digital works from private copyright owners.[27] Instead, Congress is currently considering legislation of a very different sort.

## II. THE PROPOSED ANTI-TAMPERING LAW

The National Information Infrastructure Copyright Protection Act ("NIICPA"),[28] introduced in both houses of Congress in September 1995, represents an attempt to set "rules of the road" for use of and access to copyrighted works in cyberspace.[29] The provisions of the NIICPA are taken verbatim from a "White Paper" issued by the Clinton Administration's Information Infrastructure Task Force that sets forth the Administration's position on why

---

[26]NTIA PRIVACY REPORT, *supra* note 14. The report proposes the adoption of voluntary privacy guidelines. *See infra* pp. 993, 1036-1037.

[27]Nearly all states have statutes that protect the identities and checkout records of library patrons. *See infra* note 213. Federal laws protect the privacy of video rental and cable consumers, but those protections may not cover online transactions. *See* 18 U.S.C. § 2710; 47 U.S.C. § 551; NTIA PRIVACY REPORT, *supra* note 14, at 16-17. For an overview of existing statutes that afford privacy rights to information consumers in narrower contexts, and discussion of their flaws where anonymity is concerned, see *infra* Part VI.

[28]S. 1284 & H.R. 2441, 104th Cong., 2d Sess. (1995).

[29]As of this writing, it appears that efforts to agree on a legislative markup of the original bill have failed, and that the NIICPA will not be put to a vote this year. *See* Heather Boyles, *FARNET's Washington Update* (May 17, 1996), *available online* http://www.eff.org/pub/Alerts/farnet_on_copyr_bill_960517.article. However, it is overwhelmingly certain that the bill will be reintroduced when Congress reconvenes in the fall.

changes in the existing copyright law are necessary.[30] Both the NIICPA and the NII White Paper have been analyzed in their entirety elsewhere.[31] I will focus only on section 4 of the NIICPA, which consists of a new Chapter 12, titled "Copyright Protection and Management Systems," to be added to the Copyright Act. The new chapter would establish comprehensive protection for copyright owners' decisions regarding copyright management in cyberspace.

The NIICPA's protections for copyright management systems are twofold. First, a new section 1201 of the Copyright Act would prohibit the importation, manufacture, or distribution of devices or services "the primary purpose or effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent . . . 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" of the Copyright Act.[32] Section 1202 would prohibit tampering with "copyright

---

[30]NII WHITE PAPER, *supra* note 6, app. 1.

[31]*See, e.g.*, Jessica R. Friedman, Report, *A Lawyer's Ramble Down the Information Superhighway: Copyright*, 64 FORDHAM L. REV. 705 (1995); Jessica Litman, *The Exclusive Right to Read*, 13 CARDOZO ARTS & ENT. L.J. 29 (1994); Marybeth Peters, *The Spring 1996 Horace S. Manges Lecture — The National Information Infrastructure: A Copyright Office Perspective*, 20 COLUM-VLA J.L. & ARTS 341 (1996); Samuelson, *supra* note 10; Pamela Samuelson, *Intellectual Property Rights and the Global Information Economy*, 39 COMM. OF THE ACM 23 (1996); Symposium, *Is Congress Turning the Internet into an Information Toll Road?*, INSIGHT MAG., Jan. 15, 1996, at 24 (debate between Professor James Boyle, a leading opponent of the NIICPA, and Rep. Carlos J. Moorhead, a sponsor of the bill).

[32]S. 1284 & H.R. 2441, 104th Cong., 2d Sess. § 4 (1995) (proposed § 1201 of the Copyright Act). A draft committee print prepared by the House Judiciary Committee's Subcommittee on the Courts during the unsuccessful markup negotiations, *see supra* note 29, would extend protection to any mechanism or system "an effect of which" is to prevent infringement, when there is reckless disregard of facts showing that the accused device "primarily enables such infringement." *See* Draft Committee Print of H.R. 2441 (on file with author).

management information" appended to a digital work by the copyright owner.[33] In addition to such straightforward items as the names of the author and copyright owner, "copyright management information" is defined to include "terms and conditions for uses of the work."[34] According to the NII White Paper, these provisions are needed to help copyright owners police their copyrights, in light of the otherwise trivial ease of generating and distributing unauthorized copies of their works throughout cyberspace.[35] Their combined effect is far more sweeping, and far less benign. Together, they authorize copyright owners to implement the full range of "smart" copyright management technologies described in Part I, above, and prevent readers from taking measures to protect themselves against intrusive monitoring of their activities.[36]

Proposed section 1203 provides that the anti-tampering provisions of the NIICPA are to be enforced, in the first instance, by the availability of civil damages, together with any profits earned as a result of the prohibited acts.[37] Neither the NIICPA nor the NII White Paper specifies how the damages afforded under section 1203 are to be measured. However, section 1203 does not purport to supplant section 504 of the Copyright Act, which authorizes the court to award the copyright owner "actual damages suffered . . . as a result of the infringement, and any profits of the infringer that are attributable to the infringement and are not taken into account in computing

---

[33]S. 1284 & H.R. 2441, 104th Cong., 2d Sess. § 4 (1995) (proposed § 1202 of the Copyright Act).

[34]*Id.* § 1202(c).

[35]*See* NII WHITE PAPER, note 6, at 10-12, 177-78, 230.

[36]*See* Samuelson, *supra* note 10, at 188 ("[I]n the future, it won't be possible to say no, and any effort you make to block [copyright management systems'] intrusions may make you a felon.").

[37]S. 1284 & H.R. 2441, 104th Cong., 2d Sess. § 4 (1995) (proposed § 1203 of the Copyright Act).

the actual damages."[38] This suggests that section 1203 should be interpreted as authorizing only those damages and profits attributable to the act of tampering, as distinct from damages attributable to the act of infringement, which will remain available under section 504. It is difficult to imagine how such additional damages might be quantified, which in turn suggests that section 1203, properly understood, is punitive rather than remedial in nature.

In addition to civil penalties, the NIICPA also authorizes criminal penalties for certain violations of section 1202, the provision that protects "copyright management information" against tampering.[39] Conviction under section 1204 will require a showing of "intent to defraud."[40] However, section 1204 does not state *what* the violator must have intended to defraud the copyright owner *of*. Here again, more than mere infringement seems indicated. Interpreting section 1204 to require only intent to defraud the copyright owner of the right to charge rents for the infringing use would render meaningless existing statutory provisions that already authorize criminal penalties for willful infringement.[41]

These new statutory provisions regarding copyright management systems appear intended to give copyright owners carte blanche to adopt whatever copyright management technologies

---

[38]17 U.S.C. § 504(b) (1994).

[39]S. 1284 & H.R. 2441, 104th Cong., 2d Sess. § 4 (1995) (proposed § 1204 of the Copyright Act). The draft committee print would criminalize certain violations of § 1201 as well. *See* Draft Committee Print of H.R. 2441, *supra* note 32.

[40]S. 1284 & H.R. 2441, 104th Cong., 2d Sess. § 4 (1995) (proposed § 1204 of the Copyright Act).

[41]*See* 17 U.S.C. § 506(a) (1994); 18 U.S.C. § 2319 (1994); *cf.* United States v. LaMacchia, 871 F. Supp. 535 (D. Mass. 1994) (reasoning that illegal conduct alone, without some independent source of duty to the injured party, cannot satisfy the fraud element of the federal wire fraud statute) (citing United States v. Dowling, 739 F.2d 1445, 1449-50 (9th Cir. 1984), *rev'd in part on other grounds*, 473 U.S. 207 (1985)).

they conclude will best serve their interests.[42] The NII White Paper gives only the barest of nods to the possible consequences for reader privacy and anonymity. It notes that copyright management systems "must be carefully designed and implemented to ensure that they . . . do not unduly burden use of the work by consumers or compromise their privacy."[43] Apart from this vague and fleeting show of concern, however, the NII White Paper expresses no opinion as to the types of copyright management practices that would be unduly burdensome or intrusive, and takes no position on the safeguards for reader privacy that a satisfactory system should contain. Nor does it suggest that the government should require adoption of such safeguards. The language of the NIICPA itself contains no mention of these concerns.

The Working Group on Intellectual Property Rights, which drafted the NII White Paper, was only one arm of the Information Infrastructure Task Force. The Task Force also convened a Working Group on Privacy to address questions relating to the protection of individual privacy in cyberspace.[44] The results of that effort provide little comfort, however. While the Working Group on Intellectual Property Rights came up with a detailed legislative proposal, the Working Group on Privacy compiled only a list of "principles" for both government and private industry to use in structuring future privacy policies.[45] These principles "do not have the force of law and

---

[42]*See, e.g.*, NII WHITE PAPER, *supra* note 6, at 233 ("Copyright owners should be free to determine what level or type of protection (if any) is appropriate for their works.").

[43]*Id.* at 191.

[44]U.S. Dep't of Commerce, National Telecommunications & Information Administration, *The National Information Infrastructure: Agenda For Action*, 58 FED. REG. 49,025, at 49,035 (1993).

[45]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) [hereinafter NII PRIVACY REPORT], *available online* <gopher://ntiantl.ntia.doc.gov:70/n0/papers/documents/files/niiprivprin final.html>.

do not create any substantive or procedural right enforceable at law."[46] In addition, although the NII Privacy Report expressly recognizes that "individuals should have the opportunity to remain anonymous, when appropriate,"[47] the examples it provides suggest a definition of "appropriate" that is narrow and highly deferential to the perceived needs of private copyright owners. "[B]rows[ing] a *public* electronic library" would be included[48]; by implication, browsing materials held out for purchase by a private content provider would not be considered an "appropriate" occasion for readers to assert, or take measures to protect, their anonymity rights.

A subsequent report issued by the National Telecommunications and Information Administration ("NTIA") expands upon this voluntary approach to the protection of individual privacy rights in cyberspace.[49] The NTIA Privacy Report recommends that holders of personal information adopt privacy policies based on principles of informed consent.[50] The report makes

---

[46]*Id.* at Introduction. In contrast, the European Union has adopted a directive requiring all member countries to enact laws that govern the collection, maintenance, use, and disclosure of personal data, and has designated threshold standards that such laws must meet. *See* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protesbon of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31; Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445 (1995). The European Union's Green Paper dealing with intellectual property and the global information infrastructure (the counterpart to the NII White Paper) is correspondingly more sensitive to the privacy and anonymity implications of digital copyright management systems. Commission of the European Communities, *Green Paper: Copyright and Related Rights in the Information Society* COM(95)382, 79-80 (1995) (calling for "a detailed examination" of the privacy implications of copyright management technologies); *see also* Samuelson, *supra* note 10, at 25.

[47]NII PRIVACY REPORT, *supra* note 45, at III.B., ¶ 31.

[48]NII PRIVACY REPORT, *supra* note 45, at III.B., ¶ 31.

[49]NTIA PRIVACY REPORT, *supra* note 14.

[50]NTIA PRIVACY REPORT, *supra* note 14, at 19-27. For a more detailed description of the NTIA proposal, *see infra* p. 1036-1037.

clear that its proposed notice-and-consent guidelines should be hortatory rather than mandatory.[51] Neither the Working Group's "principles" nor the NTIA's proposed guidelines provide much of a counterweight to the NIICPA's express scheme for the protection of copyright management systems, which would allow intrusions upon reader privacy and anonymity by technological fiat.

If information consumers are to be afforded meaningful protection against loss of their anonymity to intrusive copyright management practices, that protection must be found elsewhere. Before turning to that question, however, I consider whether the NIICPA and the copyright management regime it is designed to protect should be viewed as the products of an emerging societal consensus or bargain regarding the appropriate default rules for access to digital works.

## III. COPYRIGHT MANAGEMENT, PRIVATE ORDERING, AND SOCIAL CONTROL

Many commentators have hailed cyberspace as a relatively costless medium of interaction that will permit experimentation with decentralized, contract-based forms of social ordering. Some espouse the libertarian view that individuals should be free to contract, or refuse to contract, with whomever they choose and about whatever they choose without government interference.[52] Others, including many academic commentators, view such "private ordering" as

---

[51]NTIA PRIVACY REPORT, *supra* note 14 at 20-21; *see* Irving, *supra* note 12, at 260 ("[T]he plan's success depends on service providers' willingness to be self-regulating."). The report suggests that the government should mandate privacy standards only "[i]f such private sector action is not forthcoming." NTIA PRIVACY REPORT, *supra* note 14, at 21.

[52]*See, e.g.*, David D. Friedman, *Why Encryption Matters*, *available online* <http://www.best.com/~ddfr/ Libertarian/Why_Crypto_Matters.html>; Timothy C. May, *Crypto Anarchy and Virtual Communities*, *available online* <http://www.c2.org/~arkuat/consent/Anarchy.html>; Timothy C. May, *Cyphernomicon* 2.13, *available online* <http://ocaxpl.cc.oberlin.edu/~brchkind/cyphernomicon/chapter2/2.13.html>; *DigitaLiberty FAQ, available online* <http://www.digitalib.org/dl-faq.html>.

presumptively more efficient in many cases.[53] Still others favor private ordering as the antidote to "big government."[54] The NII White Paper appears to reflect a combination of these views. As described there, digital copyright management systems are a desirable and presumptively legitimate form of private ordering.[55]

Private ordering is not an unequivocal good, however, but a choice that may be acceptable or not, depending on the context. Whatever the abstract force of arguments that the law should not intervene in a functioning system of social control based on private agreements, those arguments merit little weight in the debate over how much discretion to allow copyright owners in the realm of online rights management. Among readers and copyright owners, the threads of "community" are too tenuous and the power imbalances too stark to support the conclusion that the nascent digital copyright management regime is a legitimate, bargained-for result.

Advocates of private ordering have identified several different models, any of which might plausibly provide a pattern for rulemaking in cyberspace. First, the forces of custom and community might combine to produce a system of consensual norms for governing access to copyrighted works.[56] Second, one might envision a less consensual but equally informal regime

---

[53]*See, e.g.*, Robert L. Dunne, *Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace Through A Contract Law Paradigm*, 35 JURIMETRICS J. 1 (1994); I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U. PITT. L. REV. 993 (1994); Henry H. Perritt, Jr., *Dispute Resolution in Electronic Network Communities*, 38 VILL. L. REV. 349 (1993).

[54]*See* David Kline & Daniel Burstein, *Is Government Obsolete?*, WIRED 4.01, Jan. 1996, at 86 (outlining this argument and identifying some of its proponents).

[55]NII WHITE PAPER, *supra* note 6, at 58-59, 192 n.517 (characterizing "rights management" systems simply as a form of electronic contracting).

[56]*See, e.g.*, Hardy, *supra* note 53, at 1022-24, 1036-41.

of virtual copyright management based on the freedom of individual authors and copyright owners to set terms for access to their works and the freedom of individual readers to reject those terms and purchase reading material elsewhere.[57] Finally, one might seek to understand the proposed digital copyright management regime, including the anti-tampering provisions of the NIICPA, as the result of bargaining at the interest group level. None of these models explains, much less justifies, the institution of anonymity-destroying digital copyright management systems. I address each in turn.

A leading recent study of informal private ordering suggests that, in general, systems of consensual extra-legal norms are likely to emerge among fairly well-defined, close-knit communities of repeat players.[58] In his study of dispute resolution among Shasta County, California cattle ranchers and their neighbors, Professor Ellickson found that the small, relatively self-contained community had developed its own set of internal rules for responding to property damage caused by trespassing livestock and for ensuring the construction and repair of boundary fences.[59] The parties affected by the impending digital copyright management regime exhibit none of the characteristics that Ellickson identifies as important for the development of such norms.

First, the "community" of authors, owners, and readers of copyrighted works is neither well-defined nor close-knit. It encompasses, on the one hand, giant publishing and entertainment

---

[57]*See, e.g.*, Hardy, *supra* note 53, at 1019-21, 1028-36; Perritt, *supra* note 53, at 367-72; NII WHITE PAPER, *supra* note 6, at 58-59, 192 n.517.

[58]Robert C. Ellickson, Order Without Law: How Neighbors Settle Disputes 177-206 (1991); *see also* Mark A. Lemley, *Shrinkwraps in Cyberspace*, 35 JURIMETRICS J. 311, 314 (1995).

[59]Ellickson, *supra* note 58, at 41-81, 185-89.

conglomerates such as Time-Warner and, on the other, anyone who has ever read a newspaper article or watched a movie. While all members of the copyright "community" depend on one another, in some sense, for the production, distribution, and consumption of creative works, the community's sheer size and diversity of tastes ensures that members do not depend on each other with the same immediacy as two Shasta County neighbors who share a boundary fence.[60]

A second, and related, objection is that to the extent digital copyright management systems can be said to reflect shared extra-legal norms developed by repeat-player members of a copyright "community," that community does not include readers.[61] The transient nature of the reader's interest in particular copyrighted works, compared with the more enduring interests of the authors and copyright owners in administering the rights to all of their works, marks the reader as the outsider. Ellickson offers a highway collision involving a passing tourist as an example of a situation in which Shasta County locals are content to leave adjudication of fault and determination of remedy to the legal superstructure.[62] The passing tourist has no authority to invoke the system of third-party enforcement that has arisen among neighbors who are repeat players in interactions with each other. Similarly, it is extremely unlikely that the individual

---

[60]*See* Ellickson, *supra* note 58, at 65-81, 188-89 (describing noms that govern fence construction and repair); *cf.* Perritt, *supra* note 53, at 360 (observing that the "multidimensional relationships" necessary for the development of a functioning system of extra-legal norms typically do not exist on electronic networks).

[61]*See, e.g.*, BURNS, *supra* note 5, at 59-62 (recommending that the Association of American Publishers "lead the evolution" of the digital copyright management regime); ELLICKSON, *supra* note 58, at 169 (acknowledging that some closely knit groups may have noms that maximize their own welfare at the expense of other groups); Lewis A. Komhauser, *Are There Cracks in the Foundation of Spontaneous Order?*, 67 N.Y.U. L. REV. 647, 652-55 (1992) (noting the potential problem of "exploitation of some external group," and further noting that unequal distribution of power *within* groups also may preclude formation of consensual, informal noms of the type Ellickson describes).

[62]Ellickson, *supra* note 58, at 82-103.

reader who wishes anonymous access to a copyrighted work will be able to pressure the owner to grant it by invoking shared norms that the reader helped create.

This is not to say that Ellickson's model can never be valid in cyberspace. Geographic proximity need not be the touchstone for community. Thus, for example, the model of consensual private ordering based on shared extra-legal norms may have some validity in the case of a small, inherently self-contained online discussion group. This is so because the notion of consent plays a critical role in the process of community self-definition. As a result, all members of the community will assist in enforcing the extra-legal norms that have developed within the community.[63] Members of online discussion groups have a shared interest in keeping the discussion within certain broadly defined parameters of relevance, and in making sure that fellow list members adhere to certain standards, however minimal, of courteous online behavior. Even those members who occasionally transgress group norms will assist in enforcing those rules of "netiquette" against others.[64]

It is this sense of common interest and perceived interdependence that the group composed of readers, authors, and owners of copyrighted works lacks.[65] Compelling evidence of this lack of community is the urgency with which copyright owners have supported passage of the anti-tampering provisions of the NIICPA — contrasted with the behavior of Shasta County

---

[63]Ellickson, *supra* note 58, at 207-29, 236-39.

[64]*See* Dunne, *supra* note 53, at 11; Lemley, *supra* note 58, at 313-14; Peter H. Lewis, *An Ad (Gasp!) In Cyberspace*, N.Y. TIMES, Apr. 19, 1994, at Dl. *But see* Perritt, *supra* note 53, at 360 (suggesting that the efficacy of third-party enforcement will diminish as the online population grows).

[65]*See* Perritt, *supra* note 53, at 360; *cf.* Lemley, *supra* note 58, at 314 ("Unlike e-mail discussions, or the posting of free information, commerce requires either a legal enforcement mechanism or a high degree of trust among market participants.").

residents, who simply resolved their own disputes without recourse to the legal system and often without knowledge or apparent concern as to what the law actually said.[66] The monitoring and metering capabilities now being incorporated into prototype digital copyright management systems are not community responses to isolated incidents of misbehavior by transgressors, but the unilateral, self-help response of copyright owners to the ordinary behavior of readers.[67]

---

[66]*See* Ellickson, *supra* note 58, at 48-64, 69-81. For testimony and statements in support of the NIICPA's anti-tampering provisions, see *National Information Infrastructure: Hearings on S. 1284 Before the Senate Comm. on the Judiciary*, 104th Cong., 2d Sess. (May 7, 1996) (statement 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., 2d Sess. (Feb. 7, 1996) (statements of the Association of American Publishers; Barbara A. Munder, Senior Vice President, The McGraw-Hill Companies; Frances W. Preston, President and CEO, Broadcast Music, Inc.; Jack Valenti, Chairman and Chief Executive Officer, Motion Picture Association of America, Inc.), *available in* WESTLAW, USTestimony database; Creative Incentive Coalition, *Ten Myths About the NII Copyright Protection Act* (1996), *available online* <http://www.cic.org/myths.html>; *see also On-Line Security Issues: Hearings on S /726 Before the Subcomm. on Science, Technology and Space of the Senate Comm. on Commerce*, 104th Cong., 2d Sess. (June 12, 1996) (statement of Jack Valenti Chairman and Chief Executive Officer, Motion Picture Association of America, Inc.), *available in* WESTLAW, USTestimony database.

It is also worth noting that the NIICPA's anti-tampering provisions have been opposed by a coalition of organizations representing, *inter alia*, educators and libraries; presumably, this would not be the case if the provisions merely restated a consensus. *See National Information Infrastructure: Hearings on S. 1284 Before the Senate Comm. on the Judiciary*, 104th Cong., 2d Sess. (May 7, 1996) (statement of Prof. Robert Oakley, Georgetown University Law Center, for the Digital Future Coalition), *available in* WESTLAW, USTestimony database; Digital Future Coalition, *Statement of Members of the Digital Future Coalition on H.R. 2441: The NII Copyright Protection Act of 1995* (Feb. 15, 1996), *available online* <http://www.ari.net/dfc/info/Copyright.html>. I should note that I belong to the Committee of Concerned Intellectual Property Educators, a member organization of the Digital Future Coalition.

[67]*See* Litman, *supra* note 31, at 31-32, 39 42; *cf.* Edward L. Rubin, *The Nonjudicial Life of Contract: Beyond the Shadow of the Law*, 90 NW. U.L. REV. 107, 125-31 (arguing that self-help is an important element of private ordering via contract and that repeat players enjoy "simply overwhelming" advantages in implementing the self-help strategies of their choice); *see also* Edward L. Rubin, *The Nonjudicial Life of Contract: Beyond the Shadow of the Law*, 90 NW. U. L. REV. 107, 125-31 (arguing that self-help is an important element of private ordering via contract and that repeat players enjoy "simply overwhelming" advantages in implementing

The second model of private ordering, which focuses on the cumulative effect of many arms-length transactions, would suggest that individual readers might nonetheless exert pressure on copyright owners who demand identifying information — either by bargaining for more acceptable terms or by taking their business elsewhere. If enough readers are unwilling to purchase a particular copyrighted work on the terms offered, market forces will lead the copyright owner to rethink its position. Contracts fare no better than norms in this regard, however. If copyright owners as a class adopt digital copyright management systems designed to capture readers' identities and monitor individual reading activities, it is unlikely that disgruntled readers will have any significant impact on that practice.[68]

Neither abstract notions of freedom of contract nor theories about efficient markets justify slavish adherence to contractarianism in all cases involving intellectual property rights.[69] Reader anonymity is the paradigmatic example of an issue that a contract model is ill-suited to resolve. From a purely economic standpoint, market pressures will reach high enough levels to affect particular copyright management choices only if enough individual readers conclude that the

---

the self-help strategies of their choice).

[68]There is every reason to believe that copyright owners will do so. *See* BURNS, *supra* note 5, at 59-62 (recommending that the Association of American Publishers "move as swifty as possible toward" the development of a standard for attaching usage restrictions to digital works and that it "lead the evolution" of digital copyright management technologies); Weber, *supra* note 4 (describing Copyright Clearance Center's plan to offer comprehensive digital copyright management services to member publishers); *see also On-Line Security Issues: Hearings on S. 1726 Before the Subcomm. on Science, Technology and Space of the Senate Comm. on Commerce*, 104th Cong., 2d Sess. (June 12, 1996) (statement of Jack Valenti, Chairman and Chief Executive Officer, Motion Picture Association of America, Inc.), *available online* WESTLAW, USTestimony database.

[69]*See* Lemley, *supra* note 3, at 1283-86. Professor Perritt acknowledges that contract theories based on presumed equality of bargaining power may be "artificial," and that in such situations societal norms of fairness should play a role in determining the acceptability of particular terms. Perritt, *supra* note 53, at 369-71.

benefits of withholding their custom outweigh the costs. In the particular case of a demand for reader identifying information, there is no reason to assume this is likely, and much reason to suspect the opposite. Professor Farber has argued that speech has public good characteristics that may require special protection precisely because information consumers do not accurately value the benefits of incremental speech.[70] The identical analysis applies to anonymous reading. It is difficult, if not impossible, to grant the benefits of anonymity to some individuals and withhold them from others.[71] It is also difficult to value anonymity in the abstract. Most likely, readers who seek access to "ordinary," mainstream materials for "ordinary," non-embarrassing reasons — that is, most readers in most instances — will conclude that holding out for anonymous access is not worth it. Moreover, the perceived costs of forgoing access to desired reading material will rise, and the likelihood of reader hold-out will fall, as more reading material is technologically protected. In other words, the more pervasive digital copyright management systems become, the less likely readers will be to refuse to contract with them. It is worth noting, moreover, that the anti-tampering provisions of the NIICPA, if enacted, can only decrease readers' aggregate leverage over copyright management decisions by foreclosing resistance through self-help.

If the argument that individual readers can influence copyright management decisions by withholding their business is implausible, the argument that they may seek such changes by bargaining with copyright owners one-on-one is, quite simply, absurd. First, the whole point of a digital copyright management regime is to eliminate the per-transaction bargaining that copyright

---

[70]*See* Daniel A. Farber, *Free Speech Without Romance: Public Choice and the First Amendment*, 105 HARV. L. REV. 554, 560-61 (1991).

[71]*See id.* at 558-59 (discussing attributes of public goods). Requiring eligible individuals to identify themselves to demonstrate entitlement to anonymity would defeat the purpose.

owners find so cumbersome to administer.[72] The only way to "bargain" with a digital rights management system is by hacking around it — the precise conduct that the NIICPA will prohibit. Second, and self-evidently, a right to read anonymously cannot be preserved if it must first be bargained for on a case by case basis. The act of bargaining negates the goal of concealment.[73]

Individual anonymity can be preserved, if at all, only by effective representation of readers as a group, through arms-length bargaining with the group of copyright owners — the third model of private ordering in cyberspace — or through the quasi-private, indirect bargaining characteristic of "public choice."[74] There are significant economic obstacles to collective action by readers, however. For the same reasons that most readers will simply acquiesce to the loss of anonymity on most occasions, many individuals will decide that the costs of organization

---

[72]Although some commentators have argued that the rise of electronic distribution systems will allow authors to eliminate large publishing intermediaries and transact business with readers on an individual basis. *See, e.g.*, Eugene Volokh, *Cheap Speech and What It Will Do*, 104 YALE L.J. 1805, 1834-1836 (1995); *see also* Barlow, *supra* note 5, at 126-28, the rise of digital copyright management technologies suggests precisely the opposite trend. On the information superhighway of the very near future, publishers who formerly controlled the physical plant necessary to distribute a work will administer the copyright management software that performs the equivalent function, and the bargaining position of individual readers will be, if anything, worse than before. Professor Perritt acknowledges that contract theories based on presumed equality of bargaining power may be "artificial," and that in such situations societal norms of fairness should play a role in determining the acceptability of particular terms. Perritt, *supra* note 53, at 369-71.

[73]*Cf.* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 459 (1958) ("To require that [the First Amendment right to nondisclosure of group membership] be claimed by the members themselves would result in nullification of the right at the very moment of its assertion.").

[74]*See, e.g.*, Einer R. Elhauge, *Does Interest Group Theory Justify More Intrusive Judicial Review?*, 101 YALE L.J. 31, 35-44 (1991) (defining interest group theory as based on the presumption that interest groups act to further their own welfare at the expense of other groups); *cf.* Daniel A. Farber & Philip P. Frickey, *The Jurisprudence of Public Choice*, 65 TEX. L. REV. 873, 900-01, 906-07 (1987) (arguing that a pure interest group theory does not adequately describe the legislative process, but that interest groups do "play a significant role" in that process).

outweigh the benefits.[75] It is true that some costs of collective action, particularly those associated with intra-group communication, are medium-specific. Thus, it is conceivable that in time, the ease and affordability of real-time communication in cyberspace might eliminate some of the more obvious transaction costs that might foreclose collective action by readers in the "real" world. In other contexts, the Internet has proved an unprecedentedly effective medium for harnessing collective protests by "netizens" against both government and private actions.[76] However, effective lobbying for legal change requires a far more sustained investment of effort and resources, and some real-world infrastructure to coordinate that effort.[77]

---

[75]*See* Farber, *supra* note 70, at 560-61 (discussing MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS 163-64 (1971)). Olson demonstrated that larger groups are disadvantaged in the bargaining arena because their members, each perceiving a low benefit from organization relative to its costs, will tend to free fide on the efforts of other group members, thereby reducing the group's overall strength. For a straightforward illustration of this process, *see* David McGowan & Mark A. Lemley, *Antitrust Immunity: State Action and Federalism, Petitioning and the First Amendment*, 17 HARV. J.L. & PUB. POL'Y 293, 324-25 (1994).

[76]*See, e.g.*, Sandy Close & Nick Montfort, *Free-Speech Activists in Cyberspace Gird for Virtual War*, BALTIMORE SUN, Mar. 13, 1996, at 15A (describing Internet protests against the Communications Decency Act); Jeffrey Weiss, *'24 Hours of Democracy' Puts Free Speech Protesters On Line*, DALLAS MORNING NEWS, Feb. 23, 1996, at 7A (same); *Academics Stir Internet Protest as Cambridge Press Shuns Book*, SAN DIEGO UNION-TRIB., Feb. 17, 1996, at A17 (describing protest by academic authors of publisher's decision not to publish controversial book); Associated Press, *Internet Now Home of Attack on Big Mac: McDonald's Protesters, Spurred By A 2-Year-Old Libel Trial, Have Set Up A Site on the Internet*, ORLANDO SENTINEL, Mar. 26, 1996, at B5 (describing use of Internet site to coordinate protest against McDonald's).

[77]The NIICPA itself may become a test of whether such an effort by a relatively diffuse coalition of groups and individuals can succeed. *See* Digital Future Coalition, *Statement of Members of the Digital Future Coalition on H.R. 2441: The NII Copyright Protection Act of 1995* (Feb. 15, 1996), *available online* <http://www.ari.net/dfc/info/Copyright.htm1>, *supra* note 66.

A theory of collective action also must consider whether one interest group might effectively "capture," or simply preempt, the bargaining process.[78] The institution of digital copyright management systems — an action entirely within the discretion of copyright owners to undertake or forgo — affords an excellent example of preemption. Such unilateral action renders wholly irrelevant the interest group priorities that the group of readers might assert in a hypothetical private bargaining process. The anti-tampering provisions of the NIICPA, in contrast, raise suspicions of legislative capture. Those provisions, described above, would vest copyright owners with absolute authority to define the scope of the digital rights management regime, and would make any interference with their choices illegal.[79] It is difficult to imagine a more blatant example of single-interest group legislation. Not surprisingly, publishers of copyrighted works have given the proposed law their enthusiastic support.[80]

The problem with all three models of private ordering, in short, is that the process of rule-formation may not reflect the participation of all the groups whose interests should be considered.[81] In particular, when some market participants are comparatively well-heeled and well-organized repeat players and others are not, the resulting rule — whether characterized as norm or arms-length bargain, and whether legal or extra-legal — will simply reflect the balance

---

[78]*See generally* John S. Wiley, Jr., *A Capture Theory of Antitrust Federalism*, 99 HARV. L. REV. 713, 724-26, 741-43 (1986) (outlining special interest capture theory and suggesting that it explains some, though not all, instances of government regulation).

[79]*See supra* pp. 990-92.

[80]*See supra* note 66 and accompanying text. This strong support for the proposed anti-tampering law is consistent with Professor Galanter's thesis that repeat players who have the resources to do so will seek to shape the formal rules of play in ways that favor their interests. *See* Marc Galanter, *Why the "Haves" Come Out Ahead: Speculations on the Limits of Legal Change*, 9 L. & SOC'Y REV. 95, 98-104 (1974).

[81]*See* Kornhauser, *supra* note 61, at 652-53.

of power.[82] Professor Merges has suggested that interest-group priorities unilaterally imposed via standardized contracts may achieve such a high degree of market penetration as to amount to private legislation imposed on other, unrepresented interest groups.[83] He argues that in such cases, the contracts "'become effective instruments in the hands of powerful industrial and commercial overlords, enabling them to impose a new feudal order of their own making.'"[84] This analysis applies equally to the unilateral institution of copyright management systems — which, after all, are simply standardized adhesion contracts in digital form.[85]

In sum, "private ordering" is not a talisman, but simply a descriptor for a variety of activities that occur, to some degree, within any legal regime. When the terms and conditions of access to copyrighted works are at issue, the paradigmatic small, close-knit community of repeat players necessary for a legitimate — i.e., consensual and self-enforcing — system of "order

---

[82]*See* DANIEL A. FARBER & PHILIP P. FRICKEY, LAW AND PUBLIC CHOICE: A CRITICAL INTRODUCTION 36-37, 132-43, 146 (1991); Galanter, *supra* note 80, at 103-04, 123-24, 135; Lloyd L. Weinreb, *Custom, Law, and Pubic Policy: The INS Case as an Example for Intellectual Property*, 78 VA. L. REV. 141, 144 (1992) (arguing that theories of "spontaneous social order" merely "confirm[ ] and celebrate[ ] power").

[83]Robert P. Merges, *Intellectual Property and the Costs of Commercial Exchange: A Review Essay*, 93 MICH. L. REV. 1570, 1611-13 (1995).

[84]*Id.* at 1611 (quoting Friedrich Kessler, *Contracts of Adhesion — Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629, 640 (1943)).

[85]*See* Lemley, *supra* note 58, at 319-21. Thus, Professor Lemley observes, "this new law of the Internet would be unlike any form of legislation known to modem society. No one elected its drafters . . . . They are accountable to no one. There is no provision for varying the model code in individual cases, or for amending the code itself at popular request. Nor is there any provision for 'opting out' of this new social contract, other than by withdrawing from cyberspace." *Id.* at 321. If, as I have predicted is likely, digital copyright management systems become universal and are judged a valid, consent-based form of contracting, and if federal copyright law does not preempt inconsistent license terms, *see supra* note 3, the substantive limits that copyright law places on owners' rights may become irrelevant for all practical purposes.

without law" simply does not exist. And to the extent readers lack the ability to bargain effectively, either individually or collectively, and copyright owners possess the ability unilaterally to impose technological gateways that maximize their control over the conditions of access to copyrighted works, the resulting regime can hardly be characterized as the result of "market pressures," "interest-group bargaining," or "public choice." In the electronic copyright management regime now under construction, consumers of digital works will lose the ability to read anonymously whether they like it or not. That copyright management systems may nonetheless represent "private ordering" of a sort does not resolve — or even begin to answer — the question whether that result represents good policy or good law.[86] The remainder of this Article addresses that question.

## IV. A RIGHT TO READ ANONYMOUSLY

For the most part, First Amendment jurisprudence has defined readers' rights only incidentally. Historically, both courts and commentators have been more concerned with protecting speakers than with protecting readers. Protection of speech is, of course, the First Amendment's central, express guarantee. Until recently, however, the technological means to monitor individuals' reading habits did not exist. Thus, the questions whether the First Amendment should be read to establish a right to read and what scope to accord such a right have demanded, and received, comparatively little attention.[87] They merit a great deal of attention

---

[86]*See* Weinreb, *supra* note 82, at 143; *see also* Merges, *supra* note 83, at 1611-13 (arguing that ostensibly private but universally-adopted contract provisions may have the effect of subverting federal copyright policy and substituting private, undemocratically determined conceptions of good policy in its place).

[87]Notable exceptions are Ulrika Ekman Ault, *The FBI's Library Awareness Program: Is Big Brother Reading Over Your Shoulder?*, 65 N.Y.U. L. REV. 1532, 1540-46 (1990); William E. Lee, *The Supreme Court and the Right to Receive Expression*, 1987 SUP. CT. REV. 303; and Robert M. O'Neil, *Libraries, Liberties and the First Amendment*, 42 U. CIN. L. REV. 209 (1973).

now. In light of the new digital monitoring technologies, it is vitally important that we reexamine our understanding of reading, its relationship to speech, and its place in our jurisprudence of speech and speaker's rights. This Article begins one part of that project, by considering whether there is or should be a right of anonymous access to reading materials that are otherwise made available by willing distributors.[88] It concludes that the close interdependence between receipt and expression of information and between reading and freedom of thought make recognition of such a right sound constitutional policy.[89]

The question whether the First Amendment protects a right to read anonymously is, in essence, the question whether the textual reference to "speech" may or should be understood to encompass and shield from interference all of the modes by which we participate in the process of communication. Communication may be oral or written, and participation in a given act of communication may be active or passive.[90] It is a truism that both "active" modes of

---

For a preliminary discussion of reader anonymity in the context of digital payment systems generally, see Froomkin, *supra* note 1, at 496-503. Professor Lee's 1987 review of Supreme Court decisions demonstrated that the "right to receive" had been addressed solely on a piecemeal, ad hoc basis, and that the Court had yet to articulate a cohesive vision of the right. Nor has it done so in more recent years.

[88]The Supreme Court has repeatedly indicated that the First Amendment encompasses a right to receive information from a willing speaker. *See infra* note 137 and accompanying text. My purpose here is to examine the scope of that right. The questions whether and when there might exist an affirmative right of access to particular reading materials are subjects for another Article.

[89]Of course, a constitutional right to read anonymously will not afford protection against the actions of private copyright owners unless those actions somehow implicate state action. Part V, *infra*, addresses the state action problem.

[90]As is appropriate in an article about reading, my working definition of the nature and scope of communication is derived in part from copyright law — the body of law that grants and protects authorship rights in written speech. *See* Harper & Row Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 558 (1985) ("[T]he Framers intended copyright itself to be the engine

communication — speaking and writing — qualify as constitutional "speech." The relationship between the receipt of information and expression is less well-explored.[91]

---

of free expression."). A copyrightable work of authorship may consist of words, images, or sounds, but also may consist of "numbers, or other verbal or numerical symbols or indicia." *See* 17 U.S.C. § 101. Thus, numerical or symbolic works, like verbal works, may constitute constitutional "speech." Berstein v. U.S. Dep't of State, 922 F. Supp. 1426, 1434-36 (N.D. Cal. 1996). However, to be copyrightable, a work must be "fixed" in some tangible medium from which it is capable of being "perceived, reproduced, or otherwise communicated." 17 U.S.C. § 101. Thus, my working definition is narrow as well as broad, in that it does not take into account the debate over the communicative significance of unfixed, nonverbal acts. Thus, for example, it is not my intent to define as "reading" the experience of witnessing an act of flag-burning. Arguably, some of the conduct one witnesses may be as constitutive of individual thoughts, beliefs, and subsequent expression as anything one reads. *See infra* pp. 1007-08. Nonetheless, it is hard to imagine a limiting principle, and wholly implausible to contend that First Amendment protection extends to everything one does and sees. In my view, it is neither inconsistent nor undesirable to single out the receipt of core First Amendment communication — listening and reading (including the viewing of fixed images) — as worthy of special protection.

[91] *See supra* notes 87, 88. The debate over the extent of constitutional protection for scientific research also touches on this issue. *See, e.g.*, Richard Delgado & David R. Millen, *God, Galileo, and Government: Toward Constitutional Protection for Scientific Inquiry*, 53 WASH. L. REV. 349 (1978); Gary L. Francione, *Experimentation and the Marketplace Theory of the First Amendment*, 136 U. PA. L. REV. 417 (1987); John A. Robertson, *The Scientist's Right to Research: A Constitutional Analysis*, 51 S. CAL. L. REV. 1203 (1977). Both Professor Robertson and the team of Professor Delgado and Mr. Millen argue that scientific research should be privileged as a necessary precondition for the dissemination of scientific information. Both sets of authors rely in part on a First Amendment right to receive information, although their arguments take slightly different paths. Robertson contends that a scientist's right to receive the information necessary to conduct research derives from the public's right to receive information about the end-result of such research, and suggests that scientific information is particularly important for the public to receive. Robertson, *supra*, at 1216-25. Delgado and Millen argue that a scientist's right to receive information mirrors the more general right of all citizens to receive information on issues of public concern. Delgado & Millen, *supra*, at 382-85.

Pointing out the contingent and culturally determined nature of efforts to identify the activities that are properly considered "scientific" or "informative," Professor Francione persuasively rebuts efforts to single out scientific research for special treatment. Francione, *supra*, at 482-510. He concludes, however, that the First Amendment cannot be understood to protect *any* preconditions for speech without thereby protecting all of human conduct. *Id.* at 448, 501. As discussed in note 90, *supra*, I believe that reading can be privileged without such a risk. Unlike Delgado and Millen, however, I believe that the relationship between reading and speech is fundamental and structural; receipt of external information is an essential precondition not just for "informed" speech, but for any speech. *See infra* pp. 1007-1008.

As a matter of both historical and current practice, the distinction between "active" expression and "passive" receipt is less clear than one might suppose. From a historical perspective, the strict demarcation between speaking and reading is a relatively recent one. For much of human history, everything from stories to important business matters was transmitted orally.[92] Even after the advent of written manuscripts, the words they contained were first "read" by speaking them aloud.[93] We have come a long way from the days of medieval scribes and public readings of texts and missives. However, with the advent of electronic networks and hypertext links, expression and receipt of information are blurring once again.[94] Electronic text is dynamic; rather than following a single, linear progression, the reader is free to choose his or her own path through a network of linked material. Through this process, the reader participates in the construction of the author's message.[95] While it may be premature to speak of the demise

---

[92]*See* M.T. CLANCHY, FROM MEMORY TO WRITTEN RECORD: ENGLAND 1066-1307 at 266-93 (2d ed. 1993).

[93]*See id.* at 266-93. Only gradually did solitary, silent reading become the predominant method of using written texts.

[94]For a concise, readable introduction to the concepts of hypertext and "hypermedia," *see* JAY DAVID BOLTER, WRITING SPACE: THE COMPUTER, HYPERTEXT, AND THE HISTORY OF WRITING 21-31 (1991); *see also* M. ETHAN KATSH, LAW IN A DIGITAL WORLD 198-211 (1995).

[95]*See* BOLTER, *supra* note 94, at 59-61, 113-19; GEORGE P. LANDOW, HYPERTEXT: THE CONVERGENCE OF CONTEMPORARY CRITICAL THEORY AND TECHNOLOGY 14-17 (1992) (development of hypertext "reconceive[d] reading as an active process that involves writing"), *id.* at 88-92; *see also* Paul Roberts, *Virtual Grub Street: Sorrows of a Multimedia Hack*, 292 HARPER'S MAGAZINE 71, 75-77 (1996) ("The nexus of creativity is shifted from the writer to either the producers, who lay out the text links, or the readers, who make use of those links."); *cf.* American Civil Liberties Union v. Reno, 992 F. Supp. 824, 843-44 (E.D. Pa. 1996) ("Once one has entered cyberspace, one may engage in the dialogue that occurs there. In the argot of the medium, the receiver can and does become the content provider, and vice-versa.").

of the author,[96] the creation of at least some "speech" in cyberspace thus reflects the combined efforts of both "authors" and "readers."

The uncertain separation between speaking and reading in the digital medium is simply an external manifestation of a process that all readers and listeners undergo. Functionally, the activities of the recipient and the proponent of speech — reading/hearing and speaking/writing, respectively — are properly viewed as two halves of the same whole. Freedom of speech is an empty guarantee unless one has something — anything — to say. A central insight that both copyright and literary theory can lend to First Amendment jurisprudence is that the content of one's speech is shaped by *one's response to all* prior speech, both oral and written, to which one has been exposed.

The principle that individual expression is necessarily cumulative has a rich lineage in both copyright law and critical copyright theory. "Originality," as a prerequisite for copyright protection, is a term of art; it is well-understood that every "original" work of authorship is, in many respects, a distillation of the works that came before it.[97] The same is true of *any*

---

[96]*Compare* BOLTER, *supra* note 94, at 153-66 (suggesting that the electronic author loses direct control over the path of the text but gains the power to "manipulate the reader's time at one remove" by careful construction of textual cross-references), *with* Roberts, *supra* note 95, at 75-77 (predicting that the author will vanish in the electronic age).

[97]*See, e.g.*, Campbell v. Acuff-Rose Music, Inc., 114 S. Ct. 1164, 1169 (1994) ("Every book in literature, science and art, borrows, and must necessarily borrow, and use much which was well known and used before.") (quoting Emerson v. Davies, 8 F. Cas. 615, 619 (D. Mass. 1845) (Story, J.)); Jessica Litman, *The Public Domain*, 39 EMORY L.J. 965, 966 (1990); Robert H. Rotstein, *Beyond Metaphor: Copyright Infringement and the Fiction of the Work*, 68 CHI.-KENT L. REV. 725, 756-57 (1993); *see also* JAMES BOYLE, SHAMANS, SOFTWARE, AND SPLEENS: LAW AND THE CONSTRUCTION OF THE INFORMATION SOCIETY 54-57 (1996) (arguing that the concept of the "romantic author" is a cultural construct that conveniently obscures the extent to which so-called "original" works of authorship are based on shared, preexisting cultural referents); Peter Jaszi, *Toward A Theory of Copyright: The Metamorphoses of 'Authorship,'* 41 DUKE L.J. 455 (1991) (tracing the evolution of the "Romantic vision of 'authorship"' throughout the history of American copyright law).

expression of an idea, whether or not "fixed" enough to qualify for copyright protection.[98] Thoughts and opinions, which are the predicates to speech, cannot arise in a vacuum. Whatever their content, they are responses formed to things heard or read.[99] It is this iterative process of "speech-formation" — which determines, ultimately, both the content of one's speech and the particular viewpoint one espouses — that the First Amendment should shield from scrutiny.[100]

---

[98]*See* 17 U.S.C. § 102 (copyright subsists in "original works of authorship fixed in any tangible medium of expression").

[99]*See* 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 n.284 (1995) ("[T]he objective world receives its meaning through symbolic communication, and is, therefore, necessarily mediated by dialogic relations. Identities and ideologies are formed through dialogical interaction with shared cultural symbols." (citing MICHAEL GARDINER, THE DIALOGICS OF CRITIQUE: M.M. BAKHTIN AND THE THEORY OF IDEOLOGY (1992))); *cf.* BOLTER, *supra* note 94, at 156-57 (characterizing text as "' . . . an arena in which reader and author participate in a game of the imagination' . . . every text leaves gaps for the reader to complete" (quoting Wolfgang Iser, *The Reading Process: A Phenomenological Approach*, in JANE P. TOMPKINS, READER-RESPONSE CRITICISM: FROM FORMALISM TO POST-STRUCTURALISM 50-69 (1974))); Rotstein, *supra* note 97, at 736-37 (describing the emergence of the post-structuralist view of text as dependent upon reader interpretation).

[100]*Cf.* Elkin-Koren, *supra* note 99, at 400 (characterizing cultural and political discourse as "an ongoing process of meaning-making through communicative activities" that include both communication and interpretation of preexisting symbols or cultural signifiers). Various members of the Supreme Court appears to have recognized a weaker version of this argument. In Board of Educ., Island Trees Union Free School Dist. No. 26 v. Pico, 457 U.S. 853 (1982), three justices characterized "the right to receive ideas" as "a necessary predicate to the *recipient's* meaningful exercise of his own rights of speech, press, and political freedom." *Id.* at 867 (plurality) (emphasis in original); *see also* Kleindienst v. Mandel, 408 U.S. 753, 775 (1972) (Marshall, J., dissenting) (arguing that the freedoms to hear and to speak "are inseparable; they are two sides of the same coin"); Red Lion Broadcasting v. FCC, 395 U.S. 367, 390 (1967) (observing that members of the public have the right "to receive suitable access to social, political, esthetic, moral, and other ideas and experiences"). That is so, however, not merely because of the useful or relevant information that is conveyed, *see Pico*, 457 U.S. at 867-68 (plurality), but because without access to the universe of preexisting speech that defines our understanding of the world and our place in it, one would literally have nothing to say.

To object that comparatively few people conduct in-depth research before sharing their views on a particular topic is to miss the point.[101] *All* speech responds to prior speech of some sort. The person who expresses vigorous disapproval of Hillary Clinton after months of reading electronic bulletins on "femi-nazis" from Rush Limbaugh and subscribing to anti-feminist Usenet news groups is no different in this regard than the person who reads a judicious mixture of New York Times op-ed pieces and scholarly literature on feminism before venturing to express an opinion regarding Mrs. Clinton's conduct. When the two readers choose to express their own views, the First Amendment protects both speakers equally. Logically, that zone of protection should encompass the entire series of intellectual transactions through which they formed the opinions they ultimately chose to express. Any less protection would chill inquiry, and as a result, public discourse, concerning politically and socially controversial issues — precisely those areas where vigorous public debate is most needed, and most sacrosanct.[102]

The doctrinal groundwork for a right to read anonymously is discernible in the First Amendment jurisprudence of the McCarthy era. Even in cases that accepted some degree of government power to inquire into individual involvement with suspected communist organizations, the Supreme Court's opinions reflect a sense that individual freedom to read and think lie at the heart of the zone of activity that the First Amendment protects. Thus, for example, in *Sweezy v. New Hampshire*,[103] the Court held that New Hampshire's Attorney General could not, in the course of investigating alleged communist activities, inquire into the contents of

---

[101]The debate over scientific research falls into this error. *See supra* note 91.

[102]*See, e.g.*, McIntyre v. Ohio Elections Commission, 115 S. Ct. 1511, 1519 (1995); Mills v. Alabama, 384 U.S. 214, 218-19 (1966); New York Times v. Sullivan, 376 U.S. 254, 269-70 (1964).

[103]354 U.S. 234 (1957) (plurality).

a university professor's lectures.[104] Although no analysis commanded a majority of the Court, six Justices made clear their view that the line of questioning pursued by the state threatened a core First Amendment interest in freedom of intellectual inquiry.[105] In other cases, such as *Schneider v. Smith*,[106] the Court construed statutes empowering legislative investigation into "subversive" activities narrowly, to preclude a broad authorization to "probe the reading habits" of individuals.[107]

The most direct support for a right to read anonymously appears in *Lamont v. Postmaster General*[108] and *Stanley v. Georgia*.[109] In *Lamont*, the Court struck down a postal regulation that authorized interception of mail classified as communist propaganda and required addressees to specially notify the postal service of their desire to receive the material. The regulation invalidated in *Lamont* concerned government surveillance of the mails, rather than a more general right of anonymity. Nonetheless, the Court's reasoning supports a broader application. Writing for the Court, Justice Clark relied on the chilling effect that disclosure of individual

---

[104]*Id.* at 251-55; *id.* at 261-66 (Frankfurter, J., concurring in the judgment).

[105]*Id.* at 250-51 ("Teachers and students must always remain free to inquire, to study and to evaluate, to gain new maturity and understanding; otherwise our civilization will stagnate and die."); *see also id.* at 262 (Frankfurter, J., concurring in the result) ("For society's good — if understanding be an essential need of society — inquiries into [intellectual] problems, speculations about them, stimulation in others of reflection upon them, must be left as unfettered as possible.").

[106]390 U.S. 17 (1968).

[107]*Id.* at 24-25; *see also* United States v. Rumely, 345 U.S. 41, 46-47 (1953) (holding that statutory authority to investigate "lobbying activities" did not confer power to compel names of those who purchased political literature for subsequent distribution).

[108]381 U.S. 301 (1965).

[109]394 U.S. 557 (1969).

reading preferences would produce, and reasoned that the regulation was "almost certain to have a deterrent effect" on individuals' ability to receive reading materials of their choice.[110] Accordingly, he concluded, the regulation was "at war with the 'uninhibited, robust, and wide-open' debate and discussion that are contemplated by the First Amendment."[111]

In *Stanley,* the Court ruled that a state could not criminalize the private possession of "obscene" materials — even though it might regulate commercial distribution of the identical reading materials."[112] Justice Marshall's majority opinion characterized the state's argument as, in essence, "the assertion that the State has the right to control the moral content of a person's thoughts," and termed that objective "wholly inconsistent with the philosophy of the First Amendment."[113] Again, the opinion contains language supporting a broader right of anonymity with respect to one's choice of reading material. The Court described the right being asserted as "the right to satisfy [one's] intellectual and emotional needs in the privacy of [one's] own home" and "the right to be free from state inquiry into the contents of [one's] library."[114] This is privacy language, and has been recognized as such, but it is anonymity language as well.[115]

---

[110]*Lamont*, 381 U.S. at 307.

[111]*Id.* (quoting New York Times Co. v. Sullivan, 376 U.S. 254, 270 (1964)).

[112]*Stanley*, 394 U.S. at 563-65.

[113]*Id.* at 565-66.

[114]*Id.* at 565.

[115]*See, e.g.*, Whalen v. Roe, 429 U.S. 589, 599 n.25 (1977); Roe v. Wade, 410 U.S. 113, 152 (1973). Arguably, the right of informational privacy recognized in *Whalen* and Nixon v. Administrator of General Services, 433 U.S. 425 (1977), also could be used to protect the confidentiality of individual reading decisions, at least to an extent. *See* Froomkin, *supra* note 1, at 492-94; George P. Long, III, Note, *Who Are You? Identity and Anonymity in Cyberspace*, 55 U. PITT. L. REV. 1177, 1189-93 (1994). One recent commentary characterizes the right at issue in *Stanley* as that of "privacy of thought." *See* Claudia Tuchman, Note, *Does Privacy Have Four*

The right to read anonymously implicit in *Lamont* and *Stanley* is predicated on the likely chilling effect that exposure of a reader's tastes would have on expressive conduct, broadly understood — not only speech itself, but also the information-gathering activities that precede speech.[116] More recently, the Court has held that *Stanley*'s "zone of privacy" extends only to the home, and thus does not protect even private individuals' importation or transportation of obscene material for their personal use.[117] However, the Court also has reaffirmed *Stanley*'s First

---

*Walls? Salvaging* Stanley v. Georgia, 94 COLUM. L. REV. 2267, 2280-82 (1994). Professor Kreimer locates a right of anonymity in constitutional privacy doctrine as part of a "freedom of intimate self-definition." *See* Kreimer, *supra* note 1, at 12, 69-71. Without question, "informational privacy" and anonymity concerns are closely related. As both Kreimer and Tuchman recognize, however, a pure constitutional privacy framework alone will not justify or protect the full range of anonymity concerns. *See* Kreimer, *supra* note 1, at 69-71, 131-43 (constructing a combined privacy and First Amendment rationale for a right of anonymity with respect to intimate information and "[s]elf-regarding activities crucial to personal identity"); Tuchman, *supra*, at 2280-82 (analyzing "privacy of thought" in First Amendment terms); *see also infra* notes 216-17, at 1032-33 (discussing "anonymity" issues as a unique subset of "privacy" issues).

The Ninth Circuit's recent decision in Oregon Natural Desert Ass'n v. Bibles, 83 F.3d 1168 (9th Cir. 1996), illustrates this distinction. The case involved a Freedom of Information Act request for the names of individuals on the mailing list for a newsletter distributed by the Bureau of Land Management. The court held that the privacy rights of the affected individuals did not bar disclosure because "the majority" of them had asked to be placed on the mailing list, and because disclosure was sought in order to send newsletter recipients additional materials dealing with the same subject matter. *Id.* at 1171-73. Thus, in effect, it reasoned that a request for reading material may waive any interest in having the request kept confidential. The former type of consent should not so easily be read to imply the latter. (If the federal government funded abortions, could it be required to disclose the names of individuals who had requested information about such services, so that they could be targeted for private anti-abortion mailings?) If the court had considered First Amendment-based anonymity concerns, the result might — and, I would argue, should — have been different.

[116]*See* Ault, *supra* note 87, at 1543-46; *see also* O'Neil, *supra* note 87, at 219-20 (characterizing *Lamont* as an unconstitutional conditions case). The definitive treatment of the "chilling effect" as an independent and suffcient basis for according First Amendment protection is Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect"*, 58 B.U.L. REV. 685 (1978).

[117]*See* United States v. Twelve 200-Foot Reels of Super 8mm. Film, 413 U.S. 123 (1973); United States v. Orito, 413 U.S. 139 (1973); *see also* Osborne v. Ohio, 495 U.S. 103 (1990)

Amendment-based recognition of a right of freedom of thought and intellectual inquiry — a right that necessarily includes the freedom to read unobserved.[118] Logically, the same principles that

---

(holding *Stanley* inapplicable in cases involving the private possession of child pornography because of the compelling state interest in protecting children from being used as pornographers' subjects). *Osborne*, in particular, makes clear that a sufficiently important government interest may override whatever rights of anonymity or privacy readers have. *Osborne*, 495 U.S. at 108-10; *see infra* pp. 1026-27. For a persuasive critique of the "spatial" conception of privacy developed in the post-*Stanley* cases, see Tuchman, *supra* note 115.

The Court's focus on the privacy of the home also suggests that any right to read anonymously might apply only to digital information accessed through a home computer system — and not, for example, to information accessed using computer facilities provided by one's employer. Since many individuals (including this author) connect to the Internet via an employer-provided link, the answer to this question could significantly affect the practical extent of First Amendment protection for individual reading activity. *See, e.g.*, Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1748-49 (1995) (describing how the systems operator at a university might easily monitor users' activities). In general, employee rights against surveillance by private employers are a function of federal and state privacy law. *See, e.g.*, Julie A. Flanagan, Note, *Restricting Electronic Monitoring in the Private Workplace*, 43 DUKE L.J. 1256, 1264-71 (1994); Larry O. Gantt, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345 (1995); David Neil King, Note, *Privacy Issues in the Private-Sector Workplace: Protection from Electronic Surveillance and the Emerging "Privacy Gap"*, 67 S. CAL. L. REV. 441 (1994); Note, *Addressing New Hazards of the High Technology Workplace*, 104 HARV. L. REV. 1898 (1991). Federal and state employers are directly subject to the First Amendment, but may in some circumstances limit the exercise of employee First Amendment rights for administrative reasons; the extent of this authority has been hotly disputed. *See, e.g.*, United States v. National Treasury Employees Union, 115 S. Ct. 1003 (1995); Waters v. Churchill, 511 U.S. 1061 (1994); Rankin v. McPherson, 483 U.S. 378 (1987); Connick v. Myers, 461 U.S. 138 (1983); Pickering v. Board of Educ., 391 U.S. 563 (1967); Leslie S. Blickenstaff, *Don't Tip the Scales! The Actual Malice Standard Unjustifiably Eliminates First Amendment Protection for Public Employees' Recklessly False Statements*, 70 MINN. L. REV. 2911 (1996). The question whether current law affords adequate protection to the reading activities of employees, public or private, is beyond the scope of this Article.

[118] *See* Bowers v. Hardwick, 475 U.S. 186, 195 (1986) (characterizing *Stanley* as "firmly grounded in the First Amendment['s]" prohibition against thought control); Paris Adult Theatre I v. Slaton, 413 U.S. 49, 65-67 (1973) (distinguishing refusal to protect distribution of obscene materials from "control of reason and the intellect").

forbid the state from "inquir[ing] into the contents of [one's] library" also forbid it from monitoring additions to one's library as they are acquired."[119]

The Court's recent decision in *Denver Area Educational Telecommunications Consortium, Inc. ("DAETC") v. FCC*[120] appears based in part on this reader's right of anonymity. *DAETC* concerned distribution of and access to material deemed merely indecent rather than obscene, and therefore eligible for First Amendment protection. The Court struck down a statutory provision requiring cable system operators to segregate "patently offensive" programming on a separate channel and to make that channel available to viewers only upon receipt of a written request, on the ground that the statute was more restrictive than necessary to protect minors.[121] Citing *Lamont*, the Court indicated that the First Amendment rights at stake included those of "subscribers who fear for their reputations should the operator, advertently or inadvertently, disclose the list of those who wish to watch the 'patently offensive' channel."[122] Beyond this single sentence, however, the Court offered no further discussion of the nature or extent of subscribers' First Amendment rights. The Third Circuit's opinion in *Fabulous*

---

[119]*Stanley*, 394 U.S. at 565. Whether the identical conduct by private copyright owners implicates state action sufficient to trigger First Amendment protection is discussed in Part V, *infra*.

[120]116 S. Ct. 2374 (1996).

[121]*Id.* at 2390-96. Although six members of the Court agreed that the segregation provision was unconstitutional as worded, they were divided as to the appropriate level of scrutiny. *See id.* at 2391 (suggesting that intermediate scrutiny might be required); *id.* at 2407-19 (Kennedy, J., concurring in part, concurring in the judgment in part, and dissenting in part) (arguing that strict scrutiny should apply).

[122]*Id.* at 2390 (citing Lamont v. Postmaster Gen., 381 U.S. 301, 307 (1965)). The Ninth Circuit's recent decision to require the Bureau of Land Management to disclose the names of individuals who had asked to be placed on its mailing list, though based entirely on a privacy rationale, appears inconsistent with this reasoning. *See* Oregon Natural Desert Ass'n v. Bibles, 83 F.3d 1168 (9th Cir. 1996); *supra* note 115.

*Associates, Inc. v. Pennsylvania Public Utility Commission*,[123] which invalidated Pennsylvania regulations requiring users of dial-a-porn services to preregister for personalized "access codes," contains a slightly more detailed analysis. The court reasoned that "the First Amendment protects against government 'inhibition as well as prohibition,'" including the "inhibitory effect" created by a requirement that would-be listeners identify themselves.[124]

Above and beyond the chilling effects that flow from intrusion on reader anonymity, however, such anonymity has inherent First Amendment value. Last Term, in *McIntyre v. Ohio Elections Commission*,[125] the Supreme Court reaffirmed that anonymity occupies a central place in the First Amendment lexicon. At issue was an Ohio statute that prohibited the distribution of anonymous literature designed to influence the outcome of an election. Observing that anonymous advocacy has a long and distinguished literary and political history, the Court held that an author's decision to remain anonymous is a decision about the content of his or her speech, and, as such, entitled to First Amendment protection.[126]

A similar analysis applies where reader anonymity is concerned. The freedom to read anonymously is just as much a part of our tradition, and the choice of reading materials just as expressive of identity, as the decision to use or withhold one's name. Indeed, based purely on tradition, the freedom to read anonymously may be even more fundamental than the freedom to

---

[123]896 F.2d 780 (3d Cir. 1990).

[124]*Id.* at 785 (quoting *Lamont*, 381 U.S. at 309 (Brennan, J., concurring)).

[125]115 S. Ct. 1511 (1995).

[126]*Id.* at 1516-17; *see also* Talley v. California, 362 U.S. 60, 64-65 (1960) (invalidating city ordinance prohibiting the anonymous distribution of handbills).

engage in anonymous political speech. Anonymous advocacy has always been controversial.[127] Anonymous reading, in contrast, is something that is taken for granted. The material conditions for non-anonymous reading — the technologies that enable content providers to monitor readers' activities and choices — have only recently come to exist.[128] With them has come the realization that the act of reading communicates, and that our tradition of anonymous exploration and inquiry is threatened. Reader profiles are valuable to marketers precisely because they disclose information about the reader's tastes, preferences, interests, and beliefs. That information is content that the reader should have a constitutionally protected interest in refusing to share.[129]

---

[127]*See McIntyre*, 115 S. Ct. at 1526-28 (Thomas, J., concurring) (chronicling Founding-era attempts to require authors of news articles and pamphlets to disclose their identities); *Talley*, 362 U.S. at 64-65 (describing punishments inflicted by English courts on individuals who refused to disclose information that might lead to discovery of anonymous or pseudonymous authors' identities).

[128]This terminology is borrowed from 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, 4344 (1995). Reiman defines "material conditions" for privacy as the "physical realities that hinder others in gathering information about or experiences of you." *Id.* at 43. He observes that the new monitoring technologies establish the "material conditions for invasion of privacy on unheard-of scale." *Id.* at 44. This analysis fits the particular case of copyright management technologies uncomfortably well.

The fact that nearly all states have enacted statutes to protect the confidentiality of library circulation records (low-tech and less pervasive precursors of digital copyright management systems) is compelling evidence of the high value placed by the general public on the freedom to read anonymously. *See infra* note 213.

[129]*Cf.* Anne W. Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639, 1644 (1995); Reiman, *supra* note 128, at 38-42 (arguing that such intrusions, if pervasive, will deprive individuals of "self-ownership" and stunt their inner emotional and intellectual lives). Arguably, therefore, requiring readers to disclose their identities might constitute unconstitutional compulsion. *Cf.* Wooley v. Maynard, 430 U.S. 705, 714 (1977) (holding that state motto on license plate constituted a form of compelled speech and that defendant's prosecution for removing motto violated his First Amendment rights); West Virginia Bd. of Educ. v. Barnette, 319 U.S. 624, 641 (1943) (holding that compelling public school students to recite the Pledge of Allegiance in violation of their religious beliefs offended the First Amendment).

Moreover, the most powerful justification advanced for requiring speakers to disclose their identities — an asserted need to ensure speaker accountability for harms to others resulting from defamation, harassment, and the like[130] — does not apply to readers, for the mere act of reading cannot injure.[131]

Last but not least, reading is an important dimension of the individual right of associational freedom. The Supreme Court has repeatedly held that there is a constitutionally protected right of associational anonymity.[132] As first articulated in *NAACP v. Alabama*, this protection is in part a function of the expressive aspects of association and of the chill that disclosure of unpopular associations might impose.[133] It has also been argued that a right of

---

[130]*See, e.g.*, *McIntyre*, 115 S. Ct. at 1536-37 (Scalia, J., dissenting) (arguing that speaker identification requirements are desirable because they promote accountability for false and harmful statements); Branscomb, *supra* note 129, at 1644; Froomkin, *supra* note 1, at 401-04; A. Michael Froomkin, *Anonymity and Its Enmities*, 1 J. ONLINE L. art. 4, ¶¶ 50-52 (1995), *available online* http://www.law.comell.edu/jol/froomkin.html (characterizing the accountability argument as "the strongest moral objection to the increase in anonymous interaction" on the Internet); Kreimer, *supra* note 1, at 78-88. *But see* Lee Tien, *Who's Afraid of Anonymous Speech? McIntyre and the Internet*, 75 OR. L. REV. 117, 152 (arguing that the accountability argument "ultimately reduces to a concern about ordinary individuals, not 'responsible' elites, engaging in speech without being vertically filtered").

[131]Unauthorized access to information held as a trade secret may cause injury. In such cases, anonymous access might properly be denied for other reasons. *See infra* note 149 and accompanying text.

[132]*See, e.g.*, Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539 (1963); Bates v. City of Little Rock, 361 U.S. 516 (1960); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958).

[133]*NAACP v. Alabama*, 357 U.S. at 460-62. Thus, although the Court identified the right of associational anonymity as grounded in the assembly clause of the First Amendment, it noted "the close nexus between the freedoms of speech and assembly." *Id.* at 460.

*NAACP v. Alabama* was the stated basis for the only reported First Amendment challenge to a prosecutor's attempt to subpoena library circulation records. The court summarily rejected the constitutional argument without deciding whether *NAACP* might be read to afford a right to reader anonymity. Brown v. Johnston, 328 N.W.2d 510, 512-13 (Iowa), *cert. denied*, 463 U.S. 1208 (1993).

anonymity in one's interpersonal affiliations protects the individual's right to construct his or her identity without public scrutiny.[134] Reading is intellectual association, pure and simple. As such, it is as profoundly constitutive of identity as direct interpersonal association. There are reasons for according even stronger protection to reading, moreover. Interpersonal association and group affiliation are, by definition, voluntary expressions of a common purpose or interest. Although disclosure of one's affiliations may chill protected conduct, the information revealed by such disclosure is, at least, accurate. In contrast, one may not wish to affiliate oneself with the authors of some materials one chooses to read; indeed, one may affirmatively wish otherwise. I may read *The Turner Diaries* or *The Fountainhead* for purely scholarly reasons, without any intent or desire to associate myself with the movements they have come to represent. To the extent that the dangers of being labeled by one's reading choices are greater than the dangers of being labeled by one's choice of associates, the case for First Amendment protection of association through reading is correspondingly stronger.

*Lamont* and *Stanley*, *DAETC*, *McIntyre*, and *NAACP v. Alabama* all suggest the glimmerings of judicial recognition of a broad right of anonymity extending to *all* of the constitutive activities of communication. As discussion above suggests, to describe this right as merely derivative of the First Amendment's express guarantee of freedom of speech begs the question of antecedence. While it might be correct to say that we should recognize a right to read anonymously in order to safeguard the right to speak, the activities of speaking and of receiving information are symbiotic; one cannot exist without the other, and any definition of "speech" in

---

[134] *See* Tien, *supra* note 130.

the constitutional sense properly encompasses both.[135] A First Amendment jurisprudence for the new information age should expressly reflect and affirm this broad definition. As four justices of the Supreme Court recently acknowledged, "in times of fast-changing technology," the doctrines developed "to give effect to the broad command of the First Amendment to protect speech from government interference" must be construed in light of this underlying purpose.[136] Now that digital copyright management technology has made it possible to monitor reading habits, preferences regarding political commentary, artistic tastes — in short, to intrude to an unprecedented degree on private intellectual activity of all types — the doctrines that protect "speech" must be reshaped to ensure that the protection they afford is not diminished.

Where anonymous access to privately-owned digital works is sought, however, readers' rights do not exist in a vacuum. The rights and freedoms of private copyright owners also must be considered. First, to the extent that the Supreme Court's First Amendment decisions recognize a right to read, they expressly or implicitly characterize that right as the right to receive information from a willing speaker.[137] This formulation suggests that the right to read is not

---

[135]*See* Lamont v. Postmaster Gen., 381 U.S. 301, 308 (1965) (Brennan, J., concurring) (characterizing as "equally fundamental" the rights "necessary to make the [First Amendment's] express guarantees fully meaningful").

[136]International Soc'y for Krishna Consciousness, Inc. v. Lee, 505 U.S. 672, 697 (1992) (Kennedy, J., concurring in the judgment); *see also* Denver Area Educ. Telecomm. Consonium, Inc. v. FCC, 116 S. Ct. 2374, 2402-03 (1996) (Souter, J., concurring) (analyzing the danger of establishing fixed legal standards for rapidly developing technology).

[137]*See, e.g.*, United States v. National Treasury Employees Union, 115 S. Ct. 1003, 1015 (1995); Board of Educ., Island Trees Union Free Sch. Dist. No. 26 v. Pico, 457 U.S. 853, 866-68 (plurality) (1982); Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 756-57 (1976); Kleindienst v. Mandel, 408 U.S. 753, 762-65 (1972); Red Lion Broad. Co. v. FCC, 395 U.S. 367, 390 (1969).

absolute.[138] There is no right, for example, to force information from one who is unwilling to speak.[139] The right to read, thus formulated, is the correlative of the right to speak — no narrower in scope, perhaps, but certainly no broader.[140] As a preliminary matter, then, any discussion of a right to read anonymously must consider whether an online information provider that declines to do business with an anonymous would-be customer is simply exercising its own First Amendment right not to "speak" to a unknown audience.[141]

The Supreme Court has suggested that an author's right to control the public distribution of his or her work has a constitutional dimension. In *Harper & Row, Publishers, Inc. v. Nation Enterprises*,[142] which involved the unauthorized release of excerpts from a soon-to-be-published book, the Court made clear that its refusal to invoke the fair use doctrine was motivated in part by concern for the author's First Amendment rights. The Court observed that the Framers of the Constitution "intended copyright itself to be the engine of free expression."[143] It reasoned that

---

[138]First Amendment rights assume slightly different contours where children are involved. *See, e.g.*, Sable Communications v. FCC, 492 U.S. 115, 126 (1989) (holding that children may be shielded from speech that is not "obscene" by adult standards); Tinker v. Des Moines Indep. Community Sch. Dist., 393 U.S. 503, 506 (1969) (holding that, although children do not shed their First Amendment rights at the schoolhouse door, those rights must be interpreted "in light of the special characteristics of school environment"). It is reasonable to assume that a right to read anonymously would be no different in this regard. For example, some leeway to inquire whether school children have done their assigned reading seems unwarranted. The discussion in this Article presupposes adult readers.

[139]Wooley v. Maynard, 430 U.S. 705, 714 (1977).

[140]*See* Lee, *supra* note 87, at 324-25.

[141]This formulation of the right to read also raises the question whether, in some circumstances, there might be an affirmative right of access to information that trumps the speaker's right to withhold it. This Article does not address that question.

[142]471 U.S. 539 (1985).

[143]*Id.* at 558.

copyright policies reserving control over distribution to the author serve First Amendment as well as copyright purposes. In particular, authors enjoy the same right not to speak accorded other speakers.[144] Copyright protects this right by securing to authors a right of creative control — a right not to publish ideas before they have been developed and polished to the author's satisfaction.[145]

Arguably, *Harper & Row* might be read to stand for the proposition that authors and their publishers also have a constitutionally protected right to refuse — for whatever reason — to distribute "their" works to anonymous readers.[146] However, *Harper & Row* addressed only the relatively narrow issue of the author's right to control the circumstances surrounding the first publication of a work. The reasoning that supports recognition of a First Amendment right with respect to initial publication does not necessarily indicate anything about the constitutional rights of authors and/or publishers with respect to works that have been judged ready for release and have been made available for electronic distribution.[147] For such works, the right of creative

---

[144]*Id.* at 559-60.

[145]*Id.* at 555, 559-60; *see also* Salinger v. Random House, Inc., 811 F.2d 90, 100 (2d Cir.) (holding that an author has a right "to protect the expressive content of his unpublished writings"), *cert. denied*, 484 U.S. 890 (1987).

[146]Although the right of creative control sketched by the *Harper & Row* Court might seem personal to the author, the Court did not raise this issue, but allowed a publisher to assert the right on the author's behalf. Moreover, innumerable decisions according publishers the status of First Amendment speakers make clear that publishers, too, have their own rights not to speak. *See, e.g.*, Hurley v. Irish-American Gay, Lesbian & Bisexual Group, 115 S. Ct. 2338, 2345-46 (1995); Turner Broadcasting Sys., Inc. v. FCC, 114 S. Ct. 2445, 2456 (1994); Miami Herald Publish. Co. v. Tomillo, 418 U.S. 241, 258 (1974).

[147]For purposes of this inquiry, it is not significant that a digital work may be the subject of regular revisions and updates after it is released to the general public. The dispositive question is not whether the work is "final," but whether some version of it is made available for acquisition by interested readers. *See* Julie E. Cohen, *Reverse Engineering and the Rise of Electronic Vigilantism: Intellectual Property Implications of "Lock-Out" Programs*,68 S. CAL.

control is no longer implicated. The only question is the terms on which the reader will be permitted to acquire a copy.[148]

One can envision circumstances in which the reader's identity might nonetheless matter a great deal to the author or publisher of a completed work. For example, the Church of Scientology might prefer that its literature be made available only to its own members. For such limited distribution works — works intended exclusively for a particular, limited audience — a right to refuse to engage in anonymous transactions makes sense.[149] The vast majority of works,

---

L. REV. 1091, 1113 (1995).

[148]*Cf.* Robert A. Kreiss, *Accessibility and Commercialization in Copyright Theory*, 43 UCLA L. REV. 1 (1995) (suggesting that public rights of access to a copyrighted work should turn on whether or not the work has been "commercialized"). Without more information as to what "commercialization" means—in particular, whether a copyright owner could argue that distribution to a small number of licensees is not enough to trigger Professor Kreiss' quid pro quo—I am not necessarily prepared to agree that commercialization should be the only criterion for access to a work. With a similar caveat, however, a commercialization or "general distribution" test provides a useful basis for assessing the plausibility of a copyright owner's claim that particular contract terms are necessary to effectuate its constitutional right not to speak.

[149]For similar reasons, it make sense to argue that in some circumstances a sender of electronic mail could refuse to "speak" to anonymous "listeners." This Article has focused primarily on more traditional works of authorship—literature, musical compositions, and so on—that are offered for public distribution online. *See* 17 U.S.C. § 102(a) (1994). In cyberspace, one method of distinguishing between such works and more conversational communications is lost, since in both cases, the medium of transmission is the same. *See, e.g.*, 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. 345, 389-90 (1995) (arguing that the new digital media "create a continuum" between modes of communication traditionally viewed as private and those traditionally viewed as public); Henry H. Perritt, Jr., *Tort Liability, the First Amendment, and Effectual Access to Electronic Networks*, 5 HARV. J.L. & TECH. 65, 67 (1992) (observing that the line of demarcation between electronic publishing and private electronic conversation is blurred). Nonetheless, it is difficult to argue that distribution of so-called traditional works via personalized electronic "communication" supports a right-not-to-speak claim. Although a novel certainly is speech in the constitutional sense, *see Harper & Row*, 471 U.S. at 558-60, in "real" (as opposed to cyber-) space, the decisions to write and publish it are separate, both temporally and logically, from later purchase-and-sale transactions with individual customers.

however, are offered to anyone who wishes to acquire them. Even works that have a limited audience because of their subject matter — for example, many scientific and technical publications — typically are made available to all who are interested. As to these "general distribution" works, the copyright owner wants identifying information for its own recordkeeping purposes, rather than because some identifying characteristic of the reader would affect its decision whether or not to distribute the work to that particular reader.[150] When an identification

---

It is worth noting, moreover, that many electronic mail conversations both "look" and "feel" more like traditional, published works in this regard. For example, posts to open-subscription Internet listservs or Usenet discussion groups are inherently public in nature—they are conversations with many listeners, most of whom remain silent and unidentified, and there are no membership restrictions. Accordingly, any attempt to use a right-not-to-speak claim to defeat anonymous access to listserv or Usenet posts would be implausible.

One way to determine whether a work or communication belongs in the "limited audience" category might be whether the information it contains qualifies as a trade secret. *See, e.g.*, RESTATEMENT (THIRD) UNFAIR COMPETITION § 39 (1995); Uniform Trade Secrets Act § 1(4). By definition, a trade secret's value inheres in its continuing secrecy, which its owner should remain free to protect. However, the requirement that a trade secret confer an *economic* advantage on its owner may be a difficult standard for some claimants to meet. *See, e.g.*, Religious Technology Ctr. v. Wollersheim, 796 F.2d 1076, 1090 (9th Cir. 1986) ("We do not accept that a trade secret can be based on the *spiritual advantage* the Church [of Scientology] believes its adherents acquire over non-adherents by using the materials in the prescribed manner." (emphasis in original)), *cert. denied*, 479 U.S. 1103 (1987). Nor is an "economic advantage" test necessarily appropriate for determining when an author-speaker may invoke First Amendment rights.

[150]Once armed with reader identifying information, some copyright owners who hold their works out for general distribution might seek to engage in price discrimination or private censorship with respect to particular individuals or groups. Whether this is a good thing, a bad thing, or a mixed blessing is a subject on which reasonable minds will differ. Charging lower rates to educators, for example, does not seem invidious. *See* Weber, *supra* note 4 (suggesting that some copyright owners may wish to implement a variable royalty schedule that, for example, charges more for commercial uses than for educational ones); *see also* Stefik, *supra* note 4, at 23 (envisioning grants of "special rights to certified librarians, researchers, and teachers"). However, one can imagine discriminatory policies that are far less benign. The economics and ethics of price discrimination and private censorship are vast topics, and I will not pursue them here. It is worth noting, though, that reliance on the market to suppress the more irrational instances of discriminatory pricing may be misplaced, for the reasons discussed in Part III, supra.

requirement serves administrative or copyright management purposes only, the copyright owner's First Amendment argument is at its weakest.

The force of the argument that the Constitution protects a copyright owner's right to require identifying information from readers, then, depends on the type of work to which it is applied. A copyright owner may prefer not to sell to nameless individuals, but in the vast majority of cases the First Amendment will not support that preference in the same way that it supports the right to control first publication.[151] When a copyright owner's desire for identifying information is motivated simply by copyright management concerns, the reader's right of anonymity should prevail.

A second and more important argument, however, is that the First Amendment can guarantee anonymous access to privately-owned works only to the extent that state action is implicated in copyright owners' efforts to deny such access. Even then, the right to read anonymously, like other First Amendment rights, may be subject to restrictions so long as the restrictions survive the appropriate level of scrutiny.[152] In *Fabulous*, for example, the Third

---

[151]Nor, as Part III demonstrates, may copyright owners fall back on arguments about freedom of contract to justify a preference for standardized electronic contracts that unconditionally require the surrender of anonymity.

[152]*See, e.g.*, Osborne v. Ohio, 495 U.S. 103, 108-10 (1990) (declining to recognize a constitutionally protected right to receive child pornography, in light of the compelling state interest in protecting children from abuse). Thus, for example, the deeply-rooted presumption that reading habits are sacrosanct coexists with another line of cases that accept without question judicial power to inquire into individual reading habits in particular circumstances. Most notably, a criminal defendant may question prospective jurors as to their choice of reading material in an effort to identify prior knowledge or bias. *See, e.g.*, United States v. Jackson, 542 F.2d 403 (7th Cir. 1976); United States v. Hearst, 466 F. Supp. 1068, 1076 (N.D. Cal. 1978), *modified*, 638 F.2d 1190 (9th Cir. 1980), *cert. denied*, 451 U.S. 938 (1981). Arguably, however, these cases stand for no more than the ordinary proposition that the government may impose rules that incidentally but evenhandedly burden the exercise of First Amendment rights for sufficiently substantial reasons. *See infra* page 1026.

Circuit had little difficulty deciding that the government interest in ensuring that pornography is not distributed to children could entail some sacrifice of anonymity on the part of adult dial-a-porn recipients.[153] It is against this background that the constitutionality of the proposed protection for anonymity-destroying copyright management efforts must be examined.

## V. THE FIRST AMENDMENT CASE AGAINST THE PROPOSED ANTI-TAMPERING LAW

The existence of a right to read anonymously, in the abstract, does little to guarantee individual readers protection against private conduct. The First Amendment affords protection only against governmental conduct that threatens reader anonymity. How, then, is the right to read anonymously triggered by the so-called "copyright management" efforts of private content providers? Quite simply, it is not — but the proposed anti-tampering provisions of the NIICPA are a different story. The proposed Chapter 12 of the Copyright Act would prohibit — and in some cases, criminalize — efforts to "remove or alter" copyright management information or to "avoid, bypass, remove, deactivate, or otherwise circumvent . . . *any* process, treatment, mechanism, or system" put in place for copyright protection.[154] On their face, these provisions would reach both the conduct of the willful infringer and that of the concerned libertarian who tampers with copyright management software only, and only to the extent necessary, to preserve

---

[153]Fabulous Assocs., Inc. v. Pennsylvania Pub. Util. Comm'n, 896 F.2d 780, 786 (3d Cir. 1990); *see also* Denver Area Educ. Telecomm. Consortium, Inc. v. FCC, 116 S. Ct. 2374, 2392 (1996) (discussing lesser restrictions imposed on cable operators and subscribers by other statutory provisions).

[154]S. 1284 & H.R. 2441, 104th Cong., 2d Sess. § 4 (1995) (proposed §§ 1201 and 1202 of the Copyright Act) (emphasis added).

his or her anonymity.[155] Arguably, enforcement of these provisions supplies the requisite government action. If so, their breadth cannot be justified by any governmental interest.

Merely using the judicial system to enforce a property right — or even a government-created quasi-property right — doesn't usually constitute state action.[156] Thus, for example, the Supreme Court has held that the federally-created nature of trademark rights does not automatically import state action into every lawsuit for trademark infringement.[157] The Court's analysis applies equally to copyright infringement actions. However, it is also well-accepted that the scope of copyright protection is limited by the First Amendment, by way of judicially-developed doctrines such as fair use and the idea/expression distinction.[158] These

---

[155]Whether the willful infringer, as well the concerned libertarian, would or should be permitted to assert an overbreadth challenge is a topic beyond the scope of this Article. For helpful discussions of the "third-party standing" aspect of the First Amendment overbreadth doctrine, see Michael C. Dorf, *Facial Challenges to State and Federal Statutes*, 46 STAN. L. REV. 235, 261-64 (1994); and Richard H. Fallon, *Making Sense of Overbreadth*, 100 YALE L.J. 853 (1991).

[156]*But see* Shelley v. Kraemer, 334 U.S. 1 (1948) (finding state action in private property owners' use of the court system to enforce racially restrictive covenant).

[157]*See* San Francisco Arts & Athletics, Inc. v. United States Olympic Comm., 483 U.S. 522, 544 (1987) ("All enforceable rights in trademarks are created by some governmental act . . . . The actions of trademark owners nevertheless remain private.").

[158]*See* Dowling v. United States, 473 U.S. 207, 216-17 (1985); Harper & Row, Publishers Inc. v. Nation Enters., 471 U.S. 539, 555-60 (1985) ("First Amendment protections . . . [are] embodied in the Copyright Act's distinction between copyrightable expression and uncopyrightable facts and ideas, and in the latitude for scholarship and comment traditionally afforded by fair use."); Los Angeles News Serv. v. Tullo, 973 F.2d 791, 795 (9th Cir. 1992); New Era Publications Int'l v. Henry Holt & Co., 873 F.2d 576, 584 (2d Cir. 1989), *cert denied*, 493 U.S. 1094 (1990); Triangle Publications, Inc. v. Knight-Ridder Newspapers, Inc., 626 F.2d 1171, 1174 (5th Cir. 1980); Religious Technology Ctr. v. Netcom On-Line Communication Serv., Inc., 907 F. Supp. 1361, 1377 (N.D. Cal. 1995); Maxtone-Grahum v. Burtchaell, 631 F. Supp. 1432, 1435 (S.D.N.Y.), *aff'd*, 803 F.2d 1253 (2d Cir. 1986), *cert. denied*, 481 U.S. 1059 (1987); *see also* Campbell v. Acuff-Rose Music, Inc., 114 S. Ct. 1164, 1171 (1994) (holding that commercial character of song parody did not create a presumption against fair use); W. Warren Hamel, Harper & Row v. The Nation: *A First Amendment Privilege for News Reporting of*

doctrines reflect a recognition that allowing certain private uses of the copyright laws would threaten constitutionally-protected interests. A finding of state action is implicit in this conclusion, and is neither far-fetched nor doctrinally unsound. Although the Constitution empowers Congress to confer and define the scope of copyright protection, and the courts to interpret the congressional mandate, neither may do so in a way that the First Amendment forbids.[159] The question, then, is how to characterize a legislative act that allows the institution of, and enforces compliance with, private copyright management regimes.

As the preceding paragraph suggests, the public/private distinction that forms the basis of state action doctrine is particularly problematic as applied to copyright law.[160] Even in the case

---

*Copyrightable Material?*, 19 COLUM. J.L. & SOC. PROBS. 253, 290-91 (1985) (arguing that the first amendment controls when copyright and free speech considerations clash); Melville B. Nimmer, *Does Copyright Abridge the First Amendment Guarantees of Free Speech and Press?*, 17 UCLA L. REV. 1180 (1970) (discussing the need to balance copyright and free speech interests). As the above quote from *Harper & Row* indicates, both the idea/expression distinction and the fair use doctrine were incorporated into the 1976 Copyright Act. *See* 17 U.S.C. §§ 102(b), 107 (1994).

Some have argued that in addition, the First Amendment should provide a separate, independent defense to charges of copyright infringement in some situations. *See, e.g.*, Robert C. Denicola, *Copyright and Free Speech: Constitutional Limitations on the Protection of Expression*, 67 CAL. L. REV. 283 (1979); *see also* Diane L. Zimmerman, *Information as Speech, Information as Goods: Some Thoughts on Marketplaces and the Bill of Rights*, 33 WM. & MARY L. REV. 665 (1992) (exploring the conflicts between the claims of authorship and those of the public domain where speech rights are concerned). This issue will become considerably more important if the courts and Congress conclude that copyright does not preempt private license terms that are inconsistent with substantive copyright policies. *See supra* notes 3, at 85.

[159]*See* Hamel, *supra* note 158, at 290-91 (observing that the First Amendment limits congressional power to define copyright just as it limits "other federal laws restricting expression"); *cf.* Cohen v. Cowles Media Co., 501 U.S. 663, 668 (1991) (application of state rule of law in a manner that restricts First Amendment freedoms constitutes state action); New York Times Co. v. Sullivan, 376 U.S. 254, 265 (1964).

[160]For general discussions of the evolution of the public/private distinction and its internal contradictions, see Paul Brest, *State Action and Liberal Theory: A Casenote on* Flagg Brothers v. Brooks, 130 U. PA. L. REV. 1296 (1982); Morton J. Horwitz, *The History of the Public/Private Distinction*, 130 U. PA. L. REV. 1423 (1982); Duncan Kennedy, *The Stages of the Decline of the*

of real property, the Supreme Court has recognized that "[o]wnership does not always mean absolute dominion," and that in some circumstances an owner's rights may "become circumscribed by the statutory and constitutional rights of those who use" the property.[161] Copyright, unlike real property, reflects a careful, expressly-drawn balance between private (author's) rights and public rights.[162] Thus, for example, the Copyright Act does not give a copyright owner the right to control a reader's private use of a lawfully acquired copy of his or her work.[163] In addition, as I have mentioned, the Act withholds copyright protection from ideas, processes, and the like, and also allows members of the public to make fair use of protected expression.[164] These public rights are intended to stimulate the creation of new copyrightable works, but they also are intended to safeguard the public's freedom of expression.[165] Any congressional act that appears to allow copyright owners to alter them at will should be carefully scrutinized. The anti-tampering provisions of the NIICPA fare poorly under such scrutiny.

---

*Public/Private Distinction*, 130 U. PA. L. REV. 1349 (1982).

[161]Marsh v. Alabama, 326 U.S. 501, 506 (1946).

[162]*See* United States v. Dowling, 473 U.S. 207, 216 (1985) ("The copyright owner, however, holds no ordinary chattel. A copyright . . . comprises a series of carefully defined and carefully delimited interests to which the law affords correspondingly exact protection."); Elkin-Koren, *supra* note 99, at 391-92; Wendy J. Gordon, An *Inquiry into the Merits of Copyright: The Challenges of Consistency, Consent, and Encouragement Theory*, 41 STAN. L. REV. 1343, 1370-71 (1989); Raymond T. Nimmer & Patricia Ann Krauthaus, *Copyright on the Information Superhighway: Requiem for a Middleweight*, 6 STAN. L. & POL'Y REV. 25, 27, 29-30 (1994).

[163]*See* 17 U.S.C. § 106 (1994) (listing the exclusive rights given to copyright owners); *id.* § 109(a); Elkin-Koren, *supra* note 99, at 391-92; Nimmer & Krauthaus, *supra* note 162, at 29-30.

[164]*See* 17 U.S.C. §§ 102(b), 107.

[165]Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 556-60 (1985); Nimmer, *supra* note 158, at 1186-93; *cf.* Elkin-Koren, *supra* note 99, at 392 ("[C]opyright doctrine mediates public interest in the production of information and the public interest in access to information.").

The NIICPA superimposes upon the existing framework of copyright and contract law an additional layer of private legislation regarding the terms and conditions of access to copyrighted works.[166] The law's effect, and apparent intent, is to ensure that these private terms are automatically honored, whatever their merits or defects as a matter of contract or copyright doctrine or policy.[167] In effect, then, the NIICPA delegates the enforcement of contracts — a core public function traditionally carried out by the judicial system — to private copyright owners.[168] In *Flagg Brothers, Inc. v. Brooks*,[169] the Supreme Court indicated that private resolution of a commercial dispute ordinarily will not implicate state action.[170] The proposed anti-tampering law, however, does not merely facilitate private ordering within an existing legal framework, but constitutes a wholesale delegation of power to both make the rules and prevent their violation. The *Flagg Brothers* Court expressly declined to hold that private dispute resolution could never run afoul of constitutional limits.[171] Arguably, a law that authorizes private re-ordering of rights

---

[166]*See supra* Part III.

[167]NII WHITE PAPER, *supra* note 6, at 233; *supra* pp. 991-993.

[168]*See* NCAA v. Tarkanian, 488 U.S. 179, 195-97 (1988); Jackson v. Metropolitan Edison Co., 419 U.S. 345, 351-52 (1974). The contract-policing function may be delegated to a private arbitrator, but only with the consent of the affected parties. As discussed in Part III, *supra*, that requirement is not met here.

[169]436 U.S. 149 (1978).

[170]*See id.* at 157, 160 n.10. Professor Tribe argues that private self-help should constitute state action in cases where such self-help is expressly authorized by law. LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW §18-5, at 1706-07 (2d ed. 1988). Thus far, the Court has not agreed.

[171]*See Flagg Bros.*, 436 U.S. at 162 n.l2 ("This is not to say that dispute resolution between creditors and debtors involves a category of human affairs that is never subject to constitutional constraints.").

defined in part by the First Amendment presents an appropriate situation for the imposition of such constraints.[172]

The anti-tampering regime established by the NIICPA is distinguishable from the private self-help at issue in *Flagg Brothers* in two ways, moreover. First, the NIICPA contains no provision that would allow an individual reader to seek a remedy for copyright management practices perceived as unfair. Rather, it appears that the anti-tampering provisions of the NIICPA will be the exclusive means afforded for mediating conflicts regarding digitally-imposed access restrictions.[173] Requirements imposed by a copyright owner's standard-form electronic contract and enforced by its copyright management software may be challenged only by violating the anti-tampering provisions, subjecting oneself to prosecution or suit, and raising the desired challenges as defenses once the machinery of official process has been set in motion.[174]

---

[172]*Cf.* Denver Area Educ. Telecomm. Consortium, Inc. v. FCC, 116 S. Ct. 2374, 2383-85 (1996) (plurality) (assuming that a statute allowing but not requiring specified private conduct may implicate the First Amendment). The argument that First Amendment considerations are woven into the fabric of copyright doctrine is, of course, also an argument in favor of finding copyright preemption of pervasive private contract terms that alter the balance between public and private that Congress and the courts have sought to maintain. *See supra* notes 3, 158.

[173]*See Flagg Bros.*, 436 U.S. at 159-62. The proposed Article 2B of the Uniform Commercial Code, an effort to set default rules for the licensing of intangibles, would allow a licensee to challenge contract terms on grounds of unconscionability, but as of this writing does not appear to authorize a licensee to raise such a challenge separately from and prior to its own breach. *See* U.C.C. § 2B-110 (Draft Revised Art. 2B 1996), *available online* http://www.lawlib.uh.edu/ucc2b/0503/0503_2b.html.

[174]As currently worded, both of the NIICPA's prohibitions against tampering generously allow a tamperer to raise the defense of authorization by law. *See* S. 1284 & H.R. 2441, 104th Cong., 2d Sess. § 4 (1995) (proposed §§ 1201 and 1202 of the Copyright Act).

Second, unlike the creditor in *Flagg Brothers,* copyright owners cannot obtain redress for violations of the proposed anti-tampering law without a government actor's assistance.[175] This is so regardless of which of the NIICPA's penalty provisions is invoked. Criminal prosecution under proposed section 1204 plainly would constitute state action.[176] Beyond dispute, the government may not prosecute individuals for engaging in constitutionally protected conduct. However, government involvement exists even in a civil action under the statute. As discussed above, the civil remedies afforded under the proposed anti-tampering law are not remedies for copyright infringement, but separate civil penalties tied to the act of "tampering" itself.[177] This penalty scheme directly implicates the government in the enforcement, as well as the authorization, of copyright owners' private contract regimes."[178]

The conclusion that the NIICPA's penalty provisions should be deemed to supply state action does not end the inquiry, however. We also must consider whether the NIICPA's restrictions on tampering concern speech at all, or merely "nonspeech" elements of readers' conduct. If the latter, they are subject to much more deferential review.[179] Thus, in *United States*

---

[175]*See Flagg Bros.*, 436 U.S. at 157, 160 n.10; *see also* Lugar v. Edmondson Oil Co., 457 U.S. 922, 941 (1982).

[176]*See supra* pp. 991-992.

[177]*See supra* p. 991.

[178]*See Lugar*, 457 U.S. at 941 ("While private misuse of a . . . statute does not describe conduct that can be attributed to the State, the procedural scheme created by the statute [which allowed a party to invoke a state official's assistance in seizing disputed property] obviously is the product of state action."); *Flagg Bros.*, 436 U.S. at 160 n.10.

[179]*See, e.g.*, Texas v. Johnson, 491 U.S. 397, 406-07 (1989); United States v. O'Brien, 391 U.S. 367, 376-77, 381-82 (1968).

*v. O'Brien*,[180] the Supreme Court held that the government's interest in maintaining a draft registration system based on registration certificates was sufficient to justify a law prohibiting mutilation or destruction of the certificates, notwithstanding any incidental limits the statute might impose on expressive conduct.[181] Arguably, tampering with copyright management systems is no different. Other federal statutes criminalize tampering with information stored on someone else's computer, and it has never been seriously argued that the First Amendment prevents their enforcement.[182]

When reader anonymity is at issue, tampering with copyright management systems to preserve that anonymity is intimately associated with the exercise of a First Amendment freedom. Nine years after *O'Brien,* in *Wooley v. Maynard*,[183] the Supreme Court held that a state could not constitutionally punish an individual for tampering with a license plate to obscure the unwanted message displayed there.[184] The Court reached this conclusion even though the statute at issue, like the statute in *O'Brien* (and like the NIICPA), "d[id] not punish only destruction engaged in for the purpose of expressing views."[185] *Wooley* reflects the Court's recognition that the proscribed *conduct* was the defendant's only means of preserving his freedom of expression. Similarly, failure to engage in the conduct necessary to preserve the freedom to read

---

[180]391 U.S. 367 (1968).

[181]*Id.* at 378-82.

[182]*See* 18 U.S.C. §§ 1030(a)(5), 2701 (1994).

[183]430 U.S. 705 (1977).

[184]*Id.* at 715-17.

[185]*O'Brien*, 391 U.S. at 375; *see Wooley*, 430 U.S. at 707 (quoting N.H. REV. STAT. ANN. § 262:27-c (Supp. 1975)).

anonymously results in its immediate, irretrievable loss. In the particular case of anonymity, then, the anti-tampering provisions of the NIICPA are inextricably bound up with the exercise of protected rights.

Restrictions on speech unrelated to the content of the burdened speech activities — as the NIICPA's anti-tampering provisions plainly are — must survive an "intermediate" level of scrutiny.[186] The case for the proposed anti-tampering law, then, rests on the proposition that the governmental interests associated with copyright management are "substantial" enough to warrant invasion of the freedom to read anonymously as a matter of course, and that the restriction imposed on that freedom "'is no greater than is essential to the furtherance of that interest.'"[187] Even the most staunch copyright protectionist should have difficulty making that argument with a straight face.

The government interest most often invoked to justify intrusive monitoring of electronic communications — a need to empower law enforcement agencies to detect signs of illicit activity[188] — is peculiarly inapt where copyright management systems are concerned. First, given that the NII White Paper expressly disclaims any intent to require copyright owners to

---

[186]Turner Broadcasting Sys. v. FCC, 114 S. Ct. 2445, 2469 (1994) (citing Ward v. Rock Against Racism, 491 U.S. 781 (1989), and United States v. O'Brien, 391 U.S. 367 (1968)). In contrast, the court in *Fabulous* applied strict scrutiny because the regulations at issue were directed specifically at pornography. Fabulous Assocs., Inc. v. Pennsylvania Pub. Util. Comm'n, 896 F.2d 780, 784-85 (3d Cir. 1990).

[187]*Turner Broadcasting Sys.*, 114 S. Ct. at 2469 (quoting United States v. O'Brien, 391 U.S. 367, 377 (1968)).

[188]*See, e.g.*, Froomkin, *supra* note 1, at 473-77 (predicting government opposition to anonymous digital cash); *see generally* Freiwald, *supra* note 1 (describing the various federal statutes that govern communications monitoring by law enforcement and analyzing the extent to which they preserve protection for individual privacy); Froomkin, *supra* note 21 (describing government efforts to implement the so-called Clipper encryption standard in order to acquire the capability to monitor encrypted private communications).

adopt digital "rights management" systems, it is hard to imagine a plausible argument that law enforcement needs justify such monitoring of readers' identities as copyright owners elect.[189] Second, access to preexisting copyrighted works that are held out to the public does not implicate "communication" of the sort that could serve as a predicate act for a conspiracy or wire fraud charge. Rather, the targeted activity is intellectual inquiry — an activity that the Supreme Court has suggested is entitled to the highest levels of First Amendment protection. To accept that the government has a substantial — or even any — need to monitor what citizens read for law enforcement reasons would negate that guarantee.[190] The government interest that supports public libraries' maintenance of patron checkout records is different and highly medium-specific. Physical libraries have a substantial interest in securing the timely return of loaned materials.[191] In cyberspace, no such interest exists, because the sender's computer retains the original file and distributes only copies.[192]

That copyright infringement may occasionally rise to a level that constitutes criminal activity does not change the government interest analysis.[193] While the government has an

---

[189]NII WHITE PAPER, *supra* note 6, at 233.

[190]Stanley v. Georgia, 394 U.S. 557, 565 (1969) ("If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch."); Schneider v. Smith, 390 U.S. 17, 24 (1968); Lamont v. Postmaster Gen., 381 U.S. 301, 307 (1967); *see also* United States v. Rumely, 345 U.S. 41, 57-58 (1953) (Douglas, J., concurring) ("Then the spectre of a government agent will look over the shoulder of everyone who reads. The purchase of a book or pamphlet today may result in a subpoena tomorrow. Fear of criticism goes with every person into the bookstall. The subtle, imponderable pressures of the orthodox lay hold.").

[191]*See* Froomkin, *supra* note 1, at 501 n.414. Professor Froomkin suggests that no such interest supports retention of old circulation records.

[192]*See* NII WHITE PAPER, *supra* note 6, at 92.

[193]*See* 17 U.S.C. § 506(a) (1994); 18 U.S.C. § 2319 (1994).

obvious interest in preventing wholesale piracy of copyrighted works, that interest is not implicated, much less threatened, by the actions of individuals who seek to acquire, lawfully but anonymously, copies of such works for their personal use. The more general government interest in protecting private quasi-property rights cannot justify routine monitoring of what people read any more than the government interest in protecting private reputations against libel or slander can justify routine monitoring or prior restraint of what people say.[194]

Even if the government interest in deterring copyright infringement were substantial enough to justify some restriction on First Amendment freedoms, however, the anti-tampering provisions of the NIICPA fail the second half of the intermediate scrutiny test. It is technically feasible to design copyright management systems that protect the underlying works without compromising reader anonymity. For example, a digital work might contain embedded software that automatically frustrates second-generation copying without reporting the attempted duplication to the copyright owner.[195] Alternatively, the system might collect fees via an anonymous payment system, or prevent the extraction of reader identifying data.[196] Thus, it is difficult to avoid the conclusion that the anti-tampering provisions of the NIICPA are broader than necessary to protect copyright owners' legitimate interests.

---

[194]*See, e.g.*, CBS, Inc. v. Davis, 114 S. Ct. 912, 914 (1994) (Blackmun, J.) (staying preliminary injunction barring publication of allegedly defamatory material, and observing that prior restraint will be allowed only in the most extraordinary circumstances, "where the evil that would result . . . is both great and certain and cannot be militated by less intrusive measures").

[195]Pursuant to the Audio Home Recording Act of 1992, Pub. L. No. 102-563, § 2, 106 Stat. 4237-40 (codified at 17 U.S.C. §§ 1001-02 (1992)), digital audio recording devices sold in the United States are already required to incorporate this "serial copy management" technology. *See supra* p. 988 and note 18.

[196]*See supra* notes 15, 16 and accompanying text.

A slightly more substantial government interest, where reading is concerned, is the interest in shielding children from "obscene" and "indecent" material. This interest has been held compelling in other contexts;[197] thus, it is certainly conceivable that it could justify some limitation on anonymous access to digital works. Here again, however, the fact that the government is not planning to require any particular copyright management schemes undercuts any such argument. And here again, mandatory disclosure of reader identities is a measure that is far more restrictive than is necessary to protect the government's interest. Obscene material is considered wholly ineligible for First Amendment protection;[198] thus, there is no need to screen readers by age or any other factor. The range of material that might be considered indecent is far too broad and uncertain to define with sufficient clarity. While it appears that some purveyors of sexually explicit material, such as the "dial-a-porn" at issue in *Fabulous,* make attempts to screen would-be customers, the term "indecent" as defined by the courts "would cover a broad range of material from contemporary films, plays and books . . . to controversial contemporary art."[199] A requirement that copyright owners attempt to identify and regulate access to such material would

---

[197]*See, e.g.*, Sable Communications v. FCC, 492 U.S. 115, 126 (1989) (recognizing a compelling government interest in "shielding minors from the influence of literature that is not obscene by adult standards"); New York v. Ferber, 458 U.S. 747, 756-62 (1982) (holding child pornography not entitled to First Amendment protection); FCC v. Pacifica, 438 U.S. 726, 733 (1978) (recognizing that certain "forms of offensive expression may be withheld from the young").

[198]*See, e.g.*, Paris Adult Theatre I v. Slaton, 413 U.S. 49, 66 (1973); Ginsberg v. New York, 390 U.S. 629, 635 (1968); Roth v. United States, 354 U.S. 476, 485 (1957).

[199]American Civil Liberties Union v. Reno, 929 F. Supp. 824, 855 (E.D. Pa. 1996) (opinion of Sloviter, J.); *see also, e.g.*, Manual Enterprises, Inc. v. Day, 370 U.S. 478, 487 (1962) (observing that applying an "indecency" rather than "obscenity" standard "might well put the American public in jeopardy of being denied access to many worthwhile works in literature science, or art").

lead inexorably to universal screening, and universal denial of anonymity to adult readers — an unacceptable result.[200]

For material distributed by commercial pornographers, moreover, it is technically feasible to design an anonymous "adult password" system, under which of-age readers might obtain passwords or certificates of majority from a reliable entity unconnected to any particular purveyor of copyrighted works.[201] The government's interest in protecting children also might support the argument that copyright owners should design copyright management systems that support screening software developed for private use. For example, publishers of digital works might be required to institute or participate in a rating system, so that parents, elementary schools, and the like could configure their own systems to deny access (or require a password for access) to materials rated above a certain level.[202] Such a "self-screening" regime would require no sacrifice of anonymity on the part of adult readers.

In sum, there is a strong argument that the anti-tampering provisions of the NIICPA encompass conduct protected by the First Amendment and, if enacted, cannot constitutionally be

---

[200]*Cf.* Denver Area Educ. Telecomm. Consortium, Inc. v. FCC, 116 S. Ct. 2374, 2393 (1996) (reiterating that government may not regulate speech in a manner that restricts adults to reading "only what is fit for children") (quoting Sable Communications v. FCC, 492 U.S. 115, 128 (1989)); *ACLU*, 929 F. Supp. at 876 (opinion of Dalzell, J.). Denial of anonymity in the interest of ensuring that would-be readers of arguably indecent material are screened as thoroughly as possible would subject adults to a level of supervision fit for children.

[201]*See ACLU*, 929 F. Supp. at 845-47 (describing available technologies but finding that it is neither technically nor economically feasible for most non-commercial organizations to use them); Froomkin, *supra* note 1, at 413-25 (describing the technology that enables creation of secure but anonymous digital signatures).

[202]*See ACLU*, 929 F. Supp. at 838-42 (finding such parental-screening systems technically feasible); Eugene Volokh, *Freedom of Speech on the Infobahn from the Listener's Perspective: Private Speech Restrictions, Libel, State Action, Harassment, and Sex*, 96 U. CHI. LEGAL F. (forthcoming 1996).

enforced against individuals who exercise technological self-help to protect their freedom to read anonymously. One might validly ask, though, where that leaves the rest of us. The right to exercise self-help where necessary to protect one's anonymity may seem cold comfort to the great majority of consumers who lack the technical wherewithal to do so. Although some commentators have argued otherwise,[203] merely alleging that the anti-tampering law chills the exercise of First Amendment rights probably will not confer standing to challenge it.[204] What, then, is the "ordinary" reader to do?

The unavailability of a direct legal challenge to the NIICPA need not mean that "ordinary" readers will be left without recourse. As the first line of defense, it is possible that readers who so choose will be able to pay for works using anonymous digital cash.[205] However, digital cash may not be acceptable to some copyright management systems - for example, systems designed to extract differential per-use royalties based on the nature of the user as well as the nature of the use.[206] In addition, it is entirely possible that the government will attempt to prohibit anonymous payment systems for law enforcement reasons.[207] Thus, it is more likely that would-be anonymous readers will seek to purchase the technological capabilities they lack, and

---

[203]Michael N. Dolich, Note, *Alleging A First Amendment "Chilling Effect" to Create A Plaintiff's Standing: A Practical Approach*, 43 DRAKE L. REV. 175 (1994); Jonathan R. Siegal, Note, *Chilling Injuries as a Basis for Standing*, 98 YALE L.J. 905 (1989); *see also* Ault, *supra* note 87, at 1547-49.

[204]*See* Carlin Communications, Inc. v. FCC, 837 F.2d 546, 557 (2d Cir.) (holding that provider of dial-a-porn services lacked standing to raise a facial overbreadth challenge to state access regulations on behalf of would-be listeners who might experience a chilling effect in the future), *cert. denied*, 488 U.S. 924 (1988).

[205]*See* Froomkin, *supra* note 1, at 459-70.

[206]*See supra* note 150.

[207]*See* Froomkin, *supra* note 1, at 473-78.

that a market for software and services will develop in response to this demand — unless copyright owners can use the NIICPA to prevent that result.

If the proposed anti-tampering law is unenforceable against so-called "tamperers" who merely seek to protect their own anonymity, however, it should be equally unenforceable against individuals who seek to market that capability, and only that capability, to others. Although litigants generally may not assert the constitutional rights of third parties, the Supreme Court has allowed such third-party standing where there are legal or practical obstacles to a direct challenge by the rights-holder, and where the relationship between the rights-holder and the litigant "suggests that the third party presumably wishes assertion of the right and that the litigant is capable of raising it effectively."[208] The Court has recognized that a right of anonymity affords a particularly compelling justification for third-party standing, because "[t]o require that it be claimed by the [rights-holders] themselves would result in nullification of the right at the very moment of its assertion."[209] And it has repeatedly allowed providers of allegedly unlawful

---

[208]TRIBE, *supra* note 170, § 3-19 at 138; *see, e.g.*, Singleton v. Wulff, 428 U.S. 106, 117-18 (1976) (allowing physician to assert his patient's constitutional right to obtain an abortion in challenge to statute denying reimbursement for abortion providers, on the ground that the patient's desire for anonymity might deter her from asserting her own rights); Eisenstadt v. Baird, 405 U.S. 438, 446 (1972) (allowing distributor of contraceptives to assert recipients' constitutional privacy rights in challenge to law banning distribution to unmarried individuals); Griswold v. Connecticut, 381 U.S. 479, 481 (1965) (allowing medical professionals who provided birth control to married couples to assert the users' constitutional privacy rights in challenge to their convictions under law forbidding such distribution); NAACP v. Alabama, 357 U.S. 449, 459 (1958) (allowing organization to assert its members' constitutional rights to anonymity as justification for withholding membership information from the state, on the ground that "[t]o require that it be claimed by the members themselves would result in nullification of the right at the very moment of its assertion"). *See generally* TRIBE, *supra* note 170, § 3-19 (discussing third-party standing doctrine).

[209]*NAACP*, 357 U.S. at 459 (allowing NAACP to assert its members' constitutional rights to associational anonymity); *see also Singleton*, 428 U.S. at 117-18 (observing that abortion patient's desire for anonymity might deter her from asserting her own privacy rights).

products or services to raise the rights of their clientele in situations where enforcement of the challenged law would effectively violate those rights by making the products or services unavailable.[210] Thus, assuming the state action hurdle is surmounted, there is no barrier to this type of third-party challenge to the NIICPA's penalty provisions. If such a challenge succeeded, "ordinary" readers might then be offered the opportunity to purchase the software or services that best fit their needs.

## VI. CLOSING THE CIRCLE: DESIGNING EFFECTIVE PROTECTION FOR READER ANONYMITY

Up to this point, I have considered only the implications of government intervention on the side of copyright owners. Government intervention in the development of digital copyright management systems could, of course, assume a very different form. Rather than penalizing legitimate and constitutionally protected individual conduct, the government could enact legislation that would outlaw intrusive, anonymity-destroying practices by copyright owners — or, at the very least, set strict controls on the permissible uses of reader identifying information. Under a law designed to protect the interests of readers as well as copyright owners, "ordinary" readers would not be forced to depend on judicial findings of state action and third-party standing, and on the outcome of a war of wits between hackers and developers of copyright management software, to secure their First Amendment freedoms.

Ample precedent for legislation of this type exists in the form of state and federal statutes enacted to protect consumer privacy in specific contexts. States and the federal government have

---

[210]Craig v. Boren, 429 U.S. 190, 195 (1976) (allowing vendors to challenge statute forbidding sale of 3.2% beer to men (but not women) between the ages of 18 and 21); *Singleton*, 428 U.S. at 117-18; *Eisenstadt*, 405 U.S. at 443-46; *Griswold*, 381 U.S. at 481; Pierce v. Society of Sisters, 268 U.S. 510, 534-35 (1925) (allowing private schools to challenge statute requiring parents to send their children to public schools); *see* TRIBE, *supra* note 170, § 3-19 at 138-39.

enacted legislation to protect the privacy of video rental records[211] and cable TV subscription records.[212] Most directly analogous, nearly all states have enacted legislation to protect the identities of library patrons.[213] These context-specific privacy statutes might serve as a starting point for the design of comprehensive federal legislation to safeguard reader anonymity.

Existing privacy statutes alone afford insufficient protection to readers of digital works, for three reasons. First, these statutes, whether federal or state, typically are narrow provisions

---

[211]*See* 18 U.S.C. § 2710 (1994); CAL. CIV. CODE § 1799.3 (West Supp. 1996); CONN. GEN. STAT. ANN. § 53-450 (West 1996); DEL. CODE ANN. tit 1l, § 925 (1995); IOWA CODE ANN. § 727.11 (West 1993) (amended 1996); MD. ANN. CODE art. 27, § 583 (Supp. 1991); MICH. STAT. ANN. § 19.418(101)-(104) (Callaghan 1990); MINN. STAT. ANN. § 3251.01-.03 (West 1995); N.H. REV. STAT. ANN. § 351-A:1 (Supp. 1994); N.Y. GEN. BUS. LAW §§ 671-673 (McKinney 1996); R.I. GEN. LAWS ANN. § 1l-18-32 (1994).

[212]*See* 47 U.S.C. § 551 (1992); CAL. PENAL CODE § 637.5 (West 1988); CONN. GEN. STAT. ANN. §§ 53-420 to 422 (West 1994); D.C. CODE ANN. § 43-1845 (1981); ILL. ANN. STAT. ch 720, para 110/3 (Smith-Hurd 1993); N.J. STAT. ANN. § 48:5A-54 to -63 (West 1969); WIS. STAT. ANN. § 134.43 (West 1989).

[213]*See* ALA. CODE § 41-8-10 (1975); ALASKA STAT. § 09.25.140 (1994); ARIZ. REV. STAT. ANN. § 41-1354 (1992); ARK. CODE ANN. §§ 13-2-2703 to -2704; CAL. GOV'T CODE § 6254(j) (West 1995); COLO. REV. STAT. § 24-90-119 (1973); CONN. GEN. STAT. ANN. § 11-25 (West 1986); D.C. CODE ANN. § 37-106.2 (1981); DEL. CODE ANN. tit. 29, § 10002(12) (1991); FLA. STAT. ANN. § 257.261 (West 1991); GA. CODE ANN. § 24-9-46 (Harrison 1994); ILL. ANN. STAT. ch 81, para 1201 (Smith-Hurd 1993); IND. CODE ANN. § 5-14-34(16) (Burns 1994); IOWA CODE ANN. § 22.7(13) (West 1995) (amended 1996); KAN. STAT. ANN. § 45-221(23) (Supp. 1995); ME. REV. STAT. ANN. tit. 27, § 121 (West 1988); MD. CODE ANN. STATE GOV'T § 10-616(e) (1993); MICH. COMP. LAWS ANN. §§ 397.601-605 (1982) (amended 1996); MINN. STAT. ANN. § 13.40 (West 1988) (amended 1996); MISS. CODE ANN. § 39-3-365 (1992); MO. ANN. STAT. §§ 182.815, -.817 (Vernon's 1986) MONT. CODE ANN. § 22-1-1101 to -1103 (1995); NEB. REV. STAT. § 84-712.05(10) (1994) (amended 1995); NEV. REV. STAT. § 239.013 (Michie 1996); N.H. REV. STAT. ANN. § 201-D:11; N.J. STAT. ANN. § 18A:73-43.2 (West 1989); N.M. STAT. ANN. § 18-9-4 to -5 (Michie 1978); N.Y. CIV. PRAC. LAW § 4509 (McKinney 1992); N.C. GEN. STAT. § 125-19 (Michie 1985); N.D. CENT. CODE § 40-38-12 (Supp. 1995); OKLA. STAT. ANN. tit. 51, § 24A.11 (West 1988); *id.* tit. 65, § 1-105 (1995); 24 PA. CONS. STAT. ANN. § 4428 (1992); R.I. GEN. LAWS § 38-2-2(21) (1956); S.C. CODE ANN. § 60-4-10 (Law. Co-Op. 1985); S.D. CODIFIED LAWS ANN. § 14-2-51 (1991); TENN. CODE ANN. §§ 10-8-101, -102 (1988); VT. STAT. ANN. tit. 1, § 317(b)(19) (1995); VA. CODE ANN. § 2.1-342(B)(8) (Michie Supp. 1994); WASH. REV. CODE ANN. § 42.17.310(1) (West Supp. 1996); W. VA. CODE § 10-1-22 (1995); WIS. STAT. ANN. § 43.30 (West Supp. 1995); WYO. STAT. § 16-4-203(d)(ix) (1977).

designed to protect privacy only in particular contexts.[214] Second, the NIICPA casts doubt on the applicability of even these specific protections in cyberspace. The example of video rental records is illustrative. When a consumer views a video made available by an online video service, which provision governs — the federal Video Privacy Protection Act, which says that a "rental" service may not keep or distribute records of that rental,[215] or the NIICPA, which provides safeguards to ensure that the owner of the copyright in the video may do so?

Third, and ultimately most important, although anonymity and privacy are closely related concepts, statutes enacted to protect privacy do not necessarily serve anonymity concerns.[216] The focus of existing privacy statutes, at least, is on making sure that consumer "personal identifying information" is not disclosed to unauthorized third parties. Yet the chilling effect on individual freedom to read and react to a work arises not only because information about one's reading habits might be shared with others, but also because it is collected at all — and because, even if

---

[214]For a more detailed discussion and critique of these ad hoc, context-specific privacy statutes, see Reidenberg, *supra* note l; Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497 (1996). Professor Reidenberg argues that United States legal protection for personal data falls far short of universally accepted standards, and that the failure to take a comprehensive approach to the privacy issues raised by collection of personal data is a significant cause of this inadequacy. *See* Reidenberg, *supra*, at 507-31.

[215]Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1994). It is unclear whether the language of this statute covers online video services. *See* NTIA PRIVACY REPORT, *supra* note 14, at 16-17.

[216]As discussed in note 115, *supra*, a constitutional right of anonymity may be grounded, at least partially, in constitutional privacy doctrine. Anonymity objectives and privacy objectives overlap substantially. Nonetheless, the term "anonymity" describes a particularly stringent variety of "privacy," and achieving true anonymity, as opposed to mere confidentiality, presents unique technological and procedural challenges.

not shared, it might be used by the entity that collected it.[217] And the legal interests that justify overriding some privacy concerns have greatly diminished force where anonymous access to reading materials is at issue.

Some existing privacy statutes provide that the entity collecting the personal identifying information may use or disclose that information, as long as such use falls within the ordinary course of its business.[218] In the context of the NIICPA, an "ordinary course of business" exception would allow a copyright owner to use reader identifying information to monitor readers' uses of reading materials they have purchased, particularly if the copyright owner has

---

[217] *Cf.* Smith, *supra* note 1, at 177 n.l55 (noting that the right of informational privacy focuses to a significant extent on the conditions for disclosure of personal identifying information rather than its initial collection). The *DAETC* Court appears to have recognized this distinction. *Cf.* Denver Area Educ. Telecomm. Consortium, Inc. v. FCC, 116 S. Ct. 2374, 2391 (1996) (acknowledging constitutionally protected subscriber interest in anonymity), with *id.* at 2430 (Thomas, J., dissenting) (characterizing fear of chilling effect as "pure hyperbole" given privacy provisions of statute). It is worth noting that the voluntary privacy principles set forth in the NII Privacy Report attempt to raise the threshold for collection of personal data, by stating that information users should "acquire only that information reasonably expected to support" activities that are either current or actually planned, and should destroy any information that no longer satisfies those criteria. NII PRIVACY REPORT, *supra* note 45, at II.A., ¶ 9. However, this standard is vague and affords no guarantees with respect to anonymity, which may easily be violated by the collection of such basic personal identifying information as the reader's name.

[218] *See, e.g.*, 18 U.S.C. § 2710(b)(2)(E) (1995) (video rental provider may disclose information "to any person if the disclosure is incident to the ordinary course of business of the video tape service provider"); 47 U.S.C. § 551(b)(2)(A) (1995) (cable operator may collect and use "information necessary to render a cable service or other service provided by the cable operator to a subscriber"); ARIZ. REV. STAT. ANN. § 41-1354.B.1 (1992) (allowing disclosure of library rental records "[i]f necessary for the reasonable operation of the library"); N.Y. GEN. BUS. LAW § 673(3)(c) (McKinney 1996) (allowing disclosure of video tape rental records "to any person if the disclosure is incident to the ordinary course of business of the video tape service provider"); *see also* NII PRIVACY REPORT, *supra* note 45, at II.A., ¶ 9 (framing data acquisition guidelines in terms of what is "reasonably expected to support" the collector's activities); *id.* at II.D., ¶¶ 21-23 (defining acceptable uses of personal data in terms of what would be compatible with individuals' "objectively reasonable contemplation," and suggesting that even for some "incompatible" uses, individual consent may fairly be implied from failure to use opt-out procedures). Professor Reidenberg predicts that such exceptions may become "major loophole[s]" in consumer privacy statutes. Reidenberg, *supra* note 214, at 219.

elected to charge on a per-use basis. Nor would such an exception necessarily prevent copyright owners *themselves* from using reader information to develop accurate customer profiles and then using those profiles to market other titles to customers. Thus, for example, one could imagine an HIV-positive individual who purchases a work on coping with AIDS and, shortly thereafter, begins to receive marketing literature from the work's publisher concerning other, similar titles — along, perhaps, with other promotional literature that tends to suggest that the publisher has assembled a fairly complete picture of the customer's tastes and intellectual interests. The chilling effect of this conduct might be considerable, but it is not something that existing privacy statutes were designed to prevent.

Privacy statutes also uniformly allow disclosure of personal identifying information to law enforcement authorities pursuant to a valid subpoena or warrant,[219] and some allow disclosure in response to civil subpoenas as well.[220] Where reader anonymity is concerned, it is difficult to imagine any justification for allowing routine civil discovery access to this information. Civil litigants should be required to make a showing of "compelling need," as they must before gaining access to other types of information that are presumptively privileged.[221]

---

[219] *See, e.g.*, 18 U.S.C. § 2710(b)(2)(C) (1995); CAL. CIV. CODE § 1799.3(b)(3), (4) (West Supp. 1996); COLO. REV. STAT. ANN. § 24-90-119(2)(c) (Supp. 1987); N.Y. GEN. BUS. LAW § 673(2)(a), (c) (McKinney 1988).

[220] *See, e.g.*, CAL. CIV. CODE § 1799.3(b)(1) (West Supp. 1996); CAL. PENAL CODE § 637.5(c) (government agencies only); COLO. REV. STAT. § 24-90-119(2)(c) (Supp. 1987).

[221] *See, e.g.*, 18 U.S.C. § 2710(b)(2)(F) (1995); N.Y. GEN. BUS. LAW §673(2)(b) (McKinney 1988). For example, FED. R. CIV. P. 45(c)(3)B) provides that before a litigant may require a nonparty to disclose a trade secret, it must show "a substantial need for the testimony or material that cannot otherwise be met without undue hardship." Similarly, FED. R. CIV. P. 26(b)(1) limit the discovery available from a party to matters that are "not privileged."

Such a "compelling need" threshold could be subject to appropriate exceptions. Like other privileged information, information about reading habits should be subject to discovery when a party has placed it at issue. For example, a copyright infringement defendant who denies

The question of law enforcement access to information about individual reading habits is more complicated. As discussed above, the justification for law enforcement access to information about digital transactions is substantially weakened when the subject of the inquiry is the public's reading habits.[222] Nonetheless, reading patterns may sometimes become relevant to an investigation;[223] therefore, complete denial of access to readers' personal identifying information is probably infeasible.[224] The real question, then, is not whether to allow law enforcement access to this information, but how much procedural protection to require.

As Professor Freiwald has demonstrated, the level of procedural protection accorded to digital communications generally has turned on whether the information sought is the content of

---

ever having seen or heard the plaintiff's copyrighted work should not be allowed to preclude the plaintiff from using appropriately tailored discovery requests to investigate the denial. In addition, a law privileging reader identifying information should not prevent relevant inquiry regarding documents read in the course and scope of employment, such as interoffice memos and reports.

[222]The rules of evidence in criminal proceedings reflect the heightened protection accorded to reading. Even when there is other evidence to support charging a particular individual with a particular crime, evidence relating to reading habits is inadmissible on the ultimate question of guilt. *See, e.g.*, United States v. Giese, 597 F.2d 1170, 1184-95 (9th Cir.) (evidence of reading habits admissible only to impeach defendant's contention that his reading materials showed him to be peaceable), *cert. denied*, 444 U.S. 979 (1979); United States v. McCrea, 583 F.2d 1083 (9th Cir. 1978).

[223]*See* Carol M. Ostrom, *Unabomber Case Gives Librarians Privacy Fits*, SEATTLE TIMES, May 1, 1996, at Al; Sue O'Brien, *Librarian's Silence Is Golden*, DENVER POST, Apr. 21, 1996, at E-01.

[224]The only reported court opinion to consider a First Amendment challenge to such disclosure rejected the constitutional arguments out of hand, citing a government interest in fair and effective law enforcement. Brown v. Johnston, 328 N.W.2d 510, 512-13 (Iowa 1983), *cert. denied*, 463 U.S. 1208 (1983). Provisions of the federal Video Privacy Protection Act that would have established privacy rights for library patrons were dropped from the proposed bill after disagreement arose regarding law enforcement access to circulation records. S. REP. NO. 100-599, 100th Cong., 2d Sess. 8 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342-1, 4342-8.

the communication or some other "communication attribute."[225] To gain access to communication contents requires a probable cause-based court order, while many stored records that reveal communication attributes may be easily accessed upon a broad showing of relevance.[226] If this two-tiered approach is retained as the universe of digital communications expands to include commercial transactions in cyberspace,[227] it is not clear how information such as the title of a purchased work — an item that reveals both the general nature of the "communication" and its content — would be classified. The federal Video Privacy Protection Act imposes a probable cause-based standard for disclosure, and also requires prior notice to the affected consumer,[228] but many other privacy statutes adopt the communication attribute model for all transaction records. Where reader anonymity is concerned, the nature of the right at stake warrants stronger protection. Reading preexisting copyrighted works — whether online or off — has no necessary nexus to conduct, and is not the sort of "communication" with which law enforcement will or should ordinarily be concerned.[229]

---

[225]*See* Freiwald, *supra* note 1, at 950-51, 953, 966-75, 994-97.

[226]*See id.* at 968 (discussing requirements for access to communication contents under Title III of the Omnibus Crime Control and Safe Streets Act of 1968); *id.* at 970-73 (discussing requirements for access to stored records reflecting communication attributes under the Electronic Communications Privacy Act of 1986); *id.* at 995, 1005-07 (discussing requirements for access to stored records reflecting communication attributes under the Digital Telephony Act of 1994).

[227]Professor Freiwald suggests that it should be abandoned, and replaced with strong protection for all aspects of digital communications. *See* Freiwald, *supra* note 1, at 1006-07, 1013-20.

[228]*See* 18 U.S.C. § 2710(b) (1995); Freiwald, *supra* note 1, at 1014-16.

[229]*See* Ostrom, *supra* note 223; *supra* pp. 1027-1028.

The voluntary "informed consent" system outlined in the NTIA Privacy Report also does not answer anonymity concerns.[230] The report recommends a two-tiered system under which personal information designated as "sensitive" may be disclosed only if the consumer expressly "opts in," but "nonsensitive" information may be disclosed unless the consumer expressly "opts out."[231] Examples of "sensitive" information include medical records, "sexual matters and orientation," personal financial information, and "political persuasion."[232] But where anonymity, rather than privacy, is the primary concern, the most "sensitive" piece of information is the consumer's name. Viewed through the lens of anonymity, a system that requires consumers individually to "opt out" of subsequent disclosure of their identities is logically incoherent.

It is possible that citizen concern with reader anonymity might lead individual states to legislate in the area of online reader anonymity, but less clear what such efforts could accomplish. Although several states have attempted to regulate activity in cyberspace, it is unclear whether states have authority to legislate regarding permissible uses of subscriber data by online information providers.[233] A state's jurisdiction stops at its boundaries, while the essential nature of online activity is that it does not.[234] Even assuming, however, that the individual states could validly enact laws designed to protect the anonymity of consumers of digital information,

---

[230]*See supra* p. 994.

[231]NTIA PRIVACY REPORT, *supra* note 14, at 25-26 & n.98. The report contemplates that consumers will receive a notice of the "opt-out" rule at the start of the relationship.

[232]NTIA PRIVACY REPORT, *supra* note 14, at 25-26 & n.98.

[233]*See, e.g.*, GA. CODE ANN. § 16-9-93.1 (prohibiting use of a false identity on the Internet); Ilana DeBare, *State Trademark Bill Ignites Net Turmoil*, SACRAMENTO BEE, Mar. 2, 1996, at Fl (describing California Senate bill intended to prohibit false use of trademarks on the Internet); Dan L. Burk, *Federalism in Cyberspace*, 28 CONN. L. REV. 4, 1095 (1996).

[234]*See* Burk, *supra* note 233.

the NIICPA might prevent such laws from having any meaningful effect. Certainly, a state could not authorize readers to exercise self-help that the NIICPA expressly prohibits.

A federal statute governing online content providers, in contrast, would create comprehensive protection for individual readers. To be most effective, such a law would prohibit outright the collection of reader identity data. However, an absolute ban is probably undesirable and may well be impracticable. For example, if customers cannot use anonymous-payor digital cash, online purchases of copyrighted works may necessarily reveal their identities. In addition, some customers may want copyright owners to maintain identifying records — for example, a classical music aficionado who wants to be notified as new digital recordings become available for purchase, and wants the copyright owner to remember that she likes instrumental works, but not opera.

More realistically, statutory protection for reader anonymity should recognize that initial collection of reader identity data may occur, but should require copyright owners to preserve an anonymous payment option for readers who desire it. As to those readers who elect a payment system that entails disclosure of identity, or who elect such disclosure for other reasons, the statute should erect near-impermeable barriers against aggregation, disclosure, use, and retention of identifying information for any purpose other than the one(s) the reader has expressly and specifically authorized. Such strong pro-reader default rules would counteract the disparities in bargaining power that exist between readers and copyright owners.[235]

---

[235] *See supra* Part III; *see also* GANDY, *supra* note 1, at 205-08 (observing that individual consumers "are contract takers rather than contract makers," and may not appreciate the consequences of blanket authorizations to disclose personal data or understand the full range of possible future costs).

First, the statute should forbid disclosure of *any* reader identifying information to *anyone* except law enforcement authorities without the reader's express, fully informed authorization — both as to each transaction or category of information disclosed (for example, a purchase of Bach's *Suites for Unaccompanied Cello* or a general preference for classical recordings) and as to each recipient of that information. The statute should allow civil litigants access to such information over the reader's objection only after the affected reader has been given notice and an opportunity to challenge the subpoena.[236] In any such proceeding, the requesting party should bear the burden of proving that its request is justified.[237] As to law enforcement authorities, the statute should accord reader identifying information the status of communication contents, and require a probable cause-based court order as a condition of access.[238]

Second, a statute designed to protect reader anonymity should substantially restrict the "ordinary course of business" exception that appears in many consumer privacy statutes.[239] Where reading is concerned, the only compelling reason to maintain consumer identity data at all is that some purchase transactions, such as credit card purchases, may take time to be completed. Plainly, when a reader elects to use a credit card, the law should not preclude the copyright owner from collecting and retaining the information necessary to protect its financial interests in the transaction in progress. Absent express, fully informed waiver by the consumer, however, the statute should prohibit the copyright owner from any other subsequent use of personal identifying

---

[236]*See, e.g.*, 18 U.S.C. § 2710(b)(2)(F) (1995); N.Y. GEN. BUS. LAW § 673(2)(b) (McKinney 1988).

[237]*See, e.g.*, 18 U.S.C. § 2710(b)(2)(F) (1995); N.Y. GEN. BUS. LAW § 673(2)(b) (McKinney 1988).

[238]*See supra* p. 1036.

[239]*See supra* p. 1035.

information, including aggregation for internal profiling purposes, and should require that the information be destroyed as soon as payment has been completed.[240] Moreover, there should be a separate waiver, or "opt in," requirement *as to each transaction*.[241] The value each individual places on anonymity may vary greatly, depending on the context. The HIV-positive classical music buff should not lose his right to read information about HIV and AIDS anonymously simply because he has asked to be notified when new classical recordings are released.

## VII. CONCLUSION

Digital copyright management systems capable of monitoring and charging for every use of a copyrighted work, no matter how de minimis, are not some remote, futuristic nightmare. Prototype systems exist now, and there is every reason to believe that actual systems will begin to appear online in the very near future. Once in place, they will enable an unprecedented degree of intrusion into and oversight of individual decisions about what to read, hear, and view. Perhaps the "reader's paradise" analogy is apt after all; in the digital age, it seems we will all be naked. In the face of this development, it is important that we rethink our assumptions about reading — its nature, its importance, and its relation to the activities of thinking and of speaking one's thoughts. This Article is intended as a first step in that direction.

I have argued that reading is so intimately connected with speech, and so expressive in its own right, that the freedom to read anonymously must be considered a right that the First Amendment protects. To the extent that the NIICPA and the copyright management regime it enshrines require readers to surrender their anonymity as a condition of access to digital works,

---

[240] *See, e.g.*, 47 U.S.C. § 551(e) (1995).

[241] Undoubtedly, some consumers will find a per-transaction waiver requirement annoying or onerous and wish to execute blanket waivers. The statute should allow these individuals to do so, but should afford them the opportunity to revoke such waivers upon request.

neither can be considered a legitimate private bargain between copyright owners and readers. Arguably, the provisions of the NIICPA that would give private copyright management systems, and private copyright management decisions, the force of law amount to unconstitutional state action, and could not be enforced against readers who tamper with copyright management systems solely to preserve their own anonymity or the anonymity of others. A far better solution, however, would be for Congress to recognize the implications of the new copyright management technologies for readers, and rethink the private copyright management regime it is on the verge of approving. As one of the "rules of the road" for the digital age, Congress should extend to *all* readers comprehensive protection against anonymity-destroying practices adopted by copyright owners.