

Chicago-Kent College of Law

Scholarly Commons @ IIT Chicago-Kent College of Law

All Faculty Scholarship

Faculty Scholarship

March 1996

Property and Innovation in the Global Information Infrastructure

Henry H. Perritt Jr.

IIT Chicago-Kent College of Law, hperritt@kentlaw.iit.edu

Follow this and additional works at: https://scholarship.kentlaw.iit.edu/fac_schol



Part of the [Internet Law Commons](#)

Recommended Citation

Henry H. Perritt Jr., *Property and Innovation in the Global Information Infrastructure*, 1996 U. Chi. Legal F. 261 (1996).

Available at: https://scholarship.kentlaw.iit.edu/fac_schol/486

This Article is brought to you for free and open access by the Faculty Scholarship at Scholarly Commons @ IIT Chicago-Kent College of Law. It has been accepted for inclusion in All Faculty Scholarship by an authorized administrator of Scholarly Commons @ IIT Chicago-Kent College of Law. For more information, please contact jwenger@kentlaw.iit.edu, ebarney@kentlaw.iit.edu.

Property and Innovation in the Global Information Infrastructure

Henry H. Perritt, Jr.[†]

At least since Blackstone and John Locke, legal and political commentators have recognized the central role that property plays in market economies and democracies. Property preserves personal autonomy and provides an incentive to produce.¹ At the same time, public uses of resources also are necessary to well-functioning modern societies. Intellectual-property law creates property interests in commodities that derive their value from the information contained therein, rather than from tangible raw materials. But when information is subject to property interests, a variety of competing interests enter into the balance between private ownership and public use.

New information technologies disrupt historic balances between these competing interests. Just as print technology gave rise to copyright concepts, just as phonograph recording and film technology required adaptation of copyright concepts developed for printers,² just as the Xerox machine necessitated reassessment of mid-twentieth-century copyright concepts,³ so also does the Internet require rethinking the role and form of intellectual property in stimulating a healthy information infrastructure, in which adequate incentives exist to create and deliver quality information.

[†] Professor of Law, Villanova University School of Law. I thank Paul Boltz and Eric Bootsma for research assistance. Some of the concepts in this article are developed more fully in Henry H. Perritt, Jr., *Law and the Information Superhighway* (John Wiley & Sons, 1995).

¹ See John Locke, *Of Civil Government, Two Treatises: Concerning the True Original Extent and End of Civil Government* 132 (J.M. Dent & Sons, 1924) ("As much land as a man tills, plants, improves, cultivates, and can use the product of, so much is his property. He by his labour does, as it were, enclose it from the common."); William Blackstone, 2 *Commentaries on the Laws of England* 4 (Callaghan & Co., 2d ed 1879) (stating that private ownership of property was essential to human development).

² See *Sony Corp. v Universal City Studios, Inc.*, 464 US 417, 430-31 nn 11-12 (1984) (noting impact of technology changes on copyright law).

³ See *Final Report of the National Commission on New Technological Uses of Copyrighted Works* 47 (National Commission on New Technological Uses of Copyrighted Works, 1978).

Threats to established balances do not, however, suggest that balance is no longer necessary. Owners of intellectual property should not be granted enlarged economic protection merely because they would like it. Users and exploiters of existing intellectual property should not be free of traditional intellectual-property restrictions just because they would like to be. Rather, intelligent appraisal of the role of property in an Internet-shaped information infrastructure should focus on the specific free riding and piracy risks created by the new technology. For example, traditional electronic-information services like CompuServe and Lexis do not present the same problems as the Internet's World Wide Web ("Web"). Traditional electronic-information services involve closed systems, within which it is relatively easy to arrange licenses between creators of content and electronic publishers. Such systems can enforce copyright by excluding potential or actual infringers. Neither traditional licensing nor infringer exclusion, however, is easy in the open-network environment of the Web. Moreover, the publisher/intermediaries in the Web usually only point to content; they do not reproduce, distribute, perform, or display the content themselves.⁴

Unless one carefully probes the implications of specific technologies and network architectures, one may be drawn into a fundamental and unnecessary alteration of the historic balance between property ownership and socially productive uses of information resources. The *White Paper* issued by the Clinton Administration in 1995⁵ falls into this trap. This Article suggests how such a trap can be avoided.

One must do more than merely appreciate the technology. One must also understand the role that the law plays in conjunction with other forms of protection for intellectual property. Intellectual-property production flourishes in many environments where legal protection is uncertain or entirely absent, such as the early days of desktop computer software development and radio

⁴ Copyright law only reserves to the copyright owner the rights to reproduce, prepare derivative works, distribute copies to the public, perform the work publicly, and to display the work publicly. 17 USC § 106 (1994).

⁵ United States Department of Commerce, Information Infrastructure Task Force, *Intellectual Property and the National Information Infrastructure: the Report of the Working Group on Intellectual Property Rights* (Sept 1995) ("White Paper"). The *White Paper* emphasizes the economic interests of originators and owners of existing intellectual property while deemphasizing the interests of intermediaries of those creators of new information value who may have a legitimate need to make use of existing information under the fair-use doctrine or otherwise. For a discussion of fair use, see *White Paper* § I.A.7 at 66.

and television broadcasting. Once one understands the specific threats posed by specific technologies, and the complex of protections available from law and other means, one may suggest legal changes, if any are needed.

This Article begins by exploring the nature of intellectual property in order to understand the difficult balance between competing private and public interests. It then explains how the Internet and other open network architectures bring new challenges to the positions of both content originators and intermediaries. Next, the Article considers a number of solutions for protecting the legitimate interests of intellectual-property owners while avoiding inappropriate threats and costs for entities that facilitate legitimate use and exploitation of information in an open information infrastructure.

This Article concludes that a combination of existing intellectual property and contract protections can sufficiently prevent gross piracy, especially when reinforced by anticipated changes in pricing and new product concepts and packaging. In addition, if Congress makes statutory changes, some new statutory protection for intermediaries may be appropriate. The Article emphasizes that copyright collectives can play a useful role in reducing transaction costs for the deployment of new types of protection based on technological limitations on unauthorized uses, technological detection of copyright and license violations, and electronic payment systems. In addition, collectives can make it feasible to express and enforce specific-use licenses.

The Article does not explore the important question of patent protection for processes in the Global Information Infrastructure ("GII"). It only mentions in passing the role that trademark and unfair-competition law can play in protecting the good will and marketing investment of those that produce information value. The Article assumes that basic governmental information, such as statutes, judicial opinions, agency rules and orders, and land records, is ineligible for intellectual-property protection.⁶

Professor Trotter Hardy's article in this volume applies the Calabresi and Melamed⁷ transaction-cost framework to property

⁶ See Henry H. Perritt, Jr., *Sources of Rights to Access Public Information*, 4 Wm & Mary Bill of Rights J 179, 197 (1995); Henry H. Perritt, Jr., *Should Local Governments Sell Local Spatial Databases Through State Monopolies?*, 35 Jurimet J 449, 459 (1995); Robert M. Gellman, *Twin Evils: Government Copyright and Copyright-Like Controls Over Government Information*, 45 Syracuse L Rev 999 (1995).

⁷ Guido Calabresi and A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 Harv L Rev 1089 (1972).

in cyberspace.⁸ Professor Hardy concludes that lower transaction costs resulting from cyberspace technology justify a shift toward property instead of liability concepts for protecting originators of information value.⁹ This Article, however, concerns a different facet of transaction costs in markets for information: the transaction costs that justify legal intervention in the first place.

I. INTELLECTUAL PROPERTY AS A LIMITED PROPERTY RIGHT

Property enjoys a special place in the ideology and law of market economies and democratic political systems. Indeed, the concept of property rights dates back to the earliest Western thinkers. For example, Aristotle expressly linked man's normative duty to pursue the "happy life" with man's ability to possess enough property to "make . . . life desirable and lacking in nothing."¹⁰ John Locke argued that ownership derives from nature itself, so that one must work on property in order to divorce it from raw nature.¹¹ Because man's relationship with nature, not with other men, imbues ownership, no one person or group of persons possesses the power to interfere with that right of ownership.¹²

A. Moral Rights in Property

Professor Margaret Radin's theory of property and personhood argues that a fundamental purpose of property is to give property owners a sense of identity, a feature so critical to an individual that rights in property must be protected by some legal framework.¹³ The paradigm of this connection between property and personhood is an heirloom or a house.¹⁴ Yet despite this intrinsic value that property presents to individuals,

⁸ See Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U Chi Legal F 217, 236.

⁹ Id at 260.

¹⁰ Aristotle, *Nicomachean Ethics* 43 (Harvard University Press, 1947).

¹¹ John Locke, *Of Civil Government, Two Treatises* 132 (J.M. Dent & Sons, 1924) (cited in note 1) ("As much land as a man tills, plants, improves, cultivates, and can use the product of, so much is his property. He by his labour does, as it were, enclose it from the common.").

¹² Locke stated that "being all equal and independent, no one ought to harm another in his life, health, liberty or possessions." Id at 119 (emphasis added).

¹³ Margaret Jane Radin, *Property and Personhood*, 34 Stan L Rev 957, 960 (1982) (stating that personhood springs from the act of becoming "bound up with an external thing").

¹⁴ Id at 959.

the possibility that some property can be easily exchanged for an identical good negates the inference that all property confers a moral or natural right.¹⁵ To accommodate the needs of individuals to maintain their sense of personhood through strong property rights and the need of society to allow the free flow of fungible goods, Professor Radin suggests that property should be thought of as a continuum.¹⁶ On this continuum, property for personhood would receive the most protective rights, and correspondingly, fungible property would receive lesser or no rights.¹⁷ Where a particular piece of property rests on this continuum depends on social consensus.¹⁸

Professor Radin's theory accommodates Europe's and America's traditional legal approaches to intellectual property.¹⁹ Europeans have long recognized the existence of a moral right to intellectual property which resembles Radin's property for personhood.²⁰

The American tradition is utilitarian,²¹ concentrating on the market for information and seeking to maximize the amount of content available to society. Under this concept, the fear is that, if authors have no property rights in their works, the incentive to create such works will be destroyed and the overall amount of information available to society will necessarily diminish. But, if authors have such strong property rights that almost no unconsented-to use is ever legal, then the information will be so

¹⁵ Id at 960. Fungible goods include cash, wedding rings in a jeweler's case, and commercial property.

¹⁶ Id at 986.

¹⁷ Radin, 34 Stan L Rev at 986 (cited in note 13). Radin described this phenomena as a "hierarchy of entitlements."

¹⁸ For example, Radin's attribution of personhood to an apartment is justified by the general feeling that "in today's society a tenant makes an apartment her home in the sense of a sanctuary." Id at 995. See also Stephen J. Schnably, *Property and Pragmatism: a Critique of Radin's Theory of Property and Personhood*, 45 Stan L Rev 347, 362 (1993) (arguing that social consensus is the basis of Radin's continuum and that this basis provides few objective standards).

¹⁹ See William Belanger, *U.S. Compliance With the Berne Convention*, 3 Geo Mason Independent L Rev 373, 375 (1995) (describing differences between civil-law moral-rights approach and common-law utilitarian approach to copyright).

²⁰ Moral rights were expressly recognized in the Berne Convention for the Protection of Literary and Artistic Works, Article 6 bis.

²¹ Dan W. Brock, *Utilitarianism*, in Tom Regan and Donald Van De Veer, eds, *And Justice for All* 217-240 (Rowman and Littlefield, 1982). Utilitarianism is defined by Dan Brock as "the moral theory that actions are morally right just in case they produce at least as good consequences as any alternative action open to a person." Id at 218. Thus, "the utilitarian principle requires . . . that the agent . . . act so as to maximize expected utility." Id at 220.

inaccessible that it might as well not exist. The proper equilibrium is achieved, not by examining the author's sense of identity, but by designing legal rules to create the largest, most accessible pool of information.²² This utilitarian standard avoids the social consensus and personal/fungible ambiguities of Radin's theory by providing a quantifiable method for balancing the competing public and private property interests.

B. Coase Theorem

Utilitarian analysis argues that intellectual property may be entirely unnecessary. Thus, it relieves the law of the need to strike any balance. The Coase theorem argues that, in the absence of transaction costs, it does not matter where law places entitlements. Parties will bargain and allocate legal rights and duties according to their economic preferences.²³ If there were no transaction costs, intellectual property would not matter. While the originator of valuable information would not have a copyright, he nevertheless would produce the information because someone who wanted to consume the information product would pay him to create it.

Transaction costs exist, however, in the real world of information-product creation, distribution, and consumption.²⁴ One

²² Richard A. Posner, *The Economics of Justice* 244 (Harvard University Press, 1981) (The "purpose of a property right . . . is to create an incentive to invest in the creation of information.").

²³ R. H. Coase, *The Problem of Social Cost*, 3 J L & Econ 1, 10 (1960). See also Guido Calabresi, *Transaction Costs, Resource Allocation and Liability Rules—A Comment*, 11 J L & Econ 67 (1968); G. Warren Nutter, *The Coase Theorem on Social Cost: A Footnote*, 11 J L & Econ 503 (1968).

²⁴ Calabresi and Melamed argue that the condition of no transaction costs

[M]ust be understood extremely broadly as involving both perfect knowledge in the absence of any impediments or costs of negotiating. Negotiation costs include, for example, the cost of excluding would-be-free loaders from the fruits of market bargains. . . . [The free loader] is the person who refuses to pay for a common part, although he wants it, because he believes that others will put in enough money to make the part available to him. . . . [T]he costs of excluding the free loader from the benefits for which he refused to pay may well be considerable . . . including the inefficiency of pricing a good, like the part once it exists, above its marginal cost in order to force the free loader to disclose his true desire to use it—thus enabling us to charge him part of the cost of establishing it initially.

Guido Calabresi and A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 Harv L Rev 1089, 1094-1095 n 13 (1972) (cited in note 7). Professor Coase himself identifies the following as possible elements of transaction cost: discovering those with whom one wishes to deal, informing people that one

type of transaction cost arises from the public-goods character of information. Public goods are those demonstrating the characteristics of nonrivalness or nonexhaustiveness, and nonexcludability.²⁵ One person's consumption of a public good neither interferes with nor excludes another person's consumption of the same good.²⁶ Hence, a public good is nonrival. It is also impossible (for a pure public good) to exclude any one person from benefiting from that good.²⁷ The classic example of a public good is a lighthouse.²⁸ The use by one ship of its benefit, its light, does not reduce the amount available for other ships. Nor can any ships be excluded from the benefits of the lighthouse if any ship has access to the light. Any ship in the lighthouse's vicinity may use its light to keep from running aground.²⁹

A private good is both rival and exclusive.³⁰ Consumption of the good excludes others from consuming the same good,³¹ and relative to a public good, it is much easier to exclude consumers from the good's benefit.³² Most of the goods and services bought and sold are private goods.³³ Gasoline, for example, is a private

wishes to deal and on what terms, conducting negotiations leading up to a bargain, drawing up the contract, and undertaking the inspection needed to make sure contract terms are being observed. Coase, 3 J L & Econ at 15 (cited in note 23).

²⁵ See Earl R. Brubaker, *Free Ride, Free Revelation, or Golden Rule?*, 18 J L & Econ 147, 148 (1975) (stating that two crucial properties distinguish goods: nonexhaustiveness and nonexcludability. "Purely non-exhaustive consumption may be regarded as the ultimate in positive eternity."). Brubaker states that "feasibility of exclusion from consumption . . . ranges along a continuum, namely, from low marginal cost to high marginal cost . . . [thus] classification of any specific good can be made according to its position along the two continua." *Id.* at 148-149. See also *Australia Office of Regulation Review and Economic Analysis of Copyright Reform* 13 & n 21 ISBN0-642-233359-4, orr@mail.indcom.gov.au (Australian Office of Regulation Review and Economic Analysis of Copyright Reform, 1995) ("[R]ights attaching to real property are the result of scarcity, while the rights attaching to the expression of ideas create scarcity.").

²⁶ Brubaker, 18 J L & Econ at 148-49 (cited in note 25).

²⁷ *Id.*

²⁸ Other examples include clean air and the protection provided by the American military. These goods are both nonrival and do not exclude any consumer from their benefit. Most public goods are either gifts of nature or provided by the government. Werner Sichel and Peter Eckstein, *Basic Economic Concepts—Macroeconomics* 259 (Rand McNally, 2d ed 1977).

²⁹ There are, however, few pure public goods. *Id.* Some public goods may take on the exclusive characteristics of a private good as their use increases to the point of congestion, when an additional person's use interferes with or excludes another person's use. *Id.* at 260. A public highway, for example, may be a public good until the point where traffic volume causes one additional motorist to exclude another motorist's use of the highway.

³⁰ *Id.* at 259.

³¹ Sichel & Eckstein, *Basic Economic Concepts* at 259 (cited in note 28).

³² *Id.*

³³ *Id.* at 260.

good because each gallon can be used by one consumer only to the exclusion of another consumer.

The nonexcludability and nonrival features of public goods threaten the ability of an original supplier of goods to recover her investment.³⁴ Nonexcludability means that she cannot systematically refuse to supply the good to nonpayers while supplying it to payers. Nonrivalness means that each customer becomes a potential competing supplier.³⁵ Thus, public goods, and goods that have some public-good characteristics, have a higher free-ride potential.³⁶ Conversely, the stronger the characterization of a product as a private good, with its commensurate increase in exclusivity, the lower the free-ride potential. A drive-in movie, for example, has public-good characteristics. It is nonrival and it is difficult to exclude viewers. Nonpaying viewers may not be able to hear the movie, but they can still see it and free ride to an extent. The same movie takes on private-good characteristics when shown in a private theater. It then becomes possible to exclude people from enjoying the movie altogether, ending the free-rider threat. Thus, as the movie takes on more private-good characteristics, its free-ride potential decreases.

A dichotomous private/public good distinction may not be helpful in determining free-ride potential since few goods are pure public goods.³⁷ An information product is not a pure public good, but rather a public good with private-good characteristics. The consumption of information does not necessarily reduce the amount available for another user's consumption and is therefore nonrival—a characteristic of a public good. Reading the informa-

³⁴ Id. Sichel and Eckstein cite the examples of a person who listens to an open-air concert or watches a baseball game through a fence, but does not pay for these services. Sichel & Eckstein, *Basic Economic Concepts* at 260 (cited in note 28). The nonexclusivity of the concert and the game allow the nonpaying consumer to enjoy the good's benefit.

³⁵ Both nonpaying consumers and competing suppliers in the situation described can be termed "free riders" or "free loaders" or "pirates." The most significant economic threat comes from competing suppliers, and it is that type of free riding on which this Article concentrates.

³⁶ The potential for a free ride exists when a competing supplier gets the benefits of the originator's investment without having to pay for it.

³⁷ Fire protection and radio signals are examples of goods that have strong public-good characteristics, but are not pure public goods. Sichel & Eckstein, *Basic Economic Concepts* at 259 (cited in note 28). It is difficult to exclude the benefits of these goods from certain community members, but those living closer to their source may enjoy them more fully than others. Id. All members of a community may enjoy protection by their local fire department, but families living across from the firehouse may be safer than those living farther away. Id. Similarly, those living closer to a radio tower may enjoy a clearer signal than others.

tion contained in this Article, for example, does not reduce the amount available for the next reader. On the other hand, a consumer can be excluded from using an information product until he pays—a characteristic of a private good. The same reader may be excluded from reading this Article until he, or a library, has purchased the book. To determine its free-ride potential, a product's public/private good features must be evaluated carefully.

Most information products are not perfect public goods because excludability is possible at some cost, depending on the technology. Indeed, even the light from the lighthouse—the classic example of a public good—may be handled as a private good in some circumstances.³⁸ When exclusion is feasible, it often represents a transaction cost both to producer and consumer. The originator must erect barriers, such as fences—electronic or otherwise—to keep nonpayers out, and consumers must deal with these barriers in order to strike a bargain. An example familiar to lawyers is the interposition of login routines before one can access Lexis/Nexis. Lexis/Nexis had to pay the cost of establishing and maintaining this login routine as a kind of fence around its information products. Consumers must pay the cost of remembering their login names and passwords and logging in each time they wish to consume some information.

The nonrival feature also represents a transaction cost, but only to the producer. The first consumer, having paid only for his consumption, can transfer a copy of the information to another consumer—or would be seller—without losing his own ability to consume. This means every consumer becomes an alternative source of supply at only the cost of copying. This transaction cost presents a challenge for the initial negotiations between originator and initial consumer to impose conditions on the consumer's transfer of a copy of the information.

Together, the transaction costs arising from nonexcludability and nonrivalness have justified the establishment of property rights, represented by traditional copyright, patent, and trademark rights.³⁹

³⁸ See Coase, *The Lighthouse in Economics*, 17 J L & Econ 357 (1974) (explaining that lighthouses in England were mainly financed by tolls collected at ports near the lighthouse).

³⁹ A fourth form of intellectual property, trade secret, is better understood as a liability rule under the analytical framework developed by Calabresi and Melamed. See Calabresi & Melamed, 85 Harv L. Rev at 1094-95 (1972) (cited in note 7) (explaining applicability of Coase theorem to property and liability rules).

C. Information and Tomatoes

As the preceding section noted, the features of information technology and networks complicate the utilitarian calculus. They are Coasian transaction costs. For example, suppose someone devotes much effort to discovering all of the servers on the Internet that contain information about China, believing that such information would be useful to businesses desiring to develop Chinese markets. He carefully collects the universal resource locators ("URLs") for the servers and the particular locations (files and directories) on the servers where the Chinese information may be found. He assembles the URLs into a logically organized set of Web pages so that anyone with access to his Web server can easily find and obtain copies of specific information about China.

The entrepreneur occupies a different economic position from someone who has, for example, grown a crop of tomatoes. Like the farmer, the Web entrepreneur can deny access to his product until he is paid. Unlike the farmer, however, the Web entrepreneur faces competition from his customers. The farmer's customer, having bought one tomato, has only one tomato. While she may resell that tomato, her resale does not deprive the farmer of anything. The farmer has already been paid. This characteristic of the tomato is "rival," signifying that two persons may fight over the tomato, but that they cannot both have exclusive possession of it.

Unfortunately for the Web entrepreneur, his products may be nonrival,⁴⁰ depending on how he packages and sells them. If he transfers the entire collection of Web pointers to each customer, the customer easily can make copies of the set of pointers and sell the copies. The nature of digital technology makes the cost of copying very low. Thus, the customer can keep what she bought and also sell one or more copies.⁴¹ The economic reward gives her an incentive to engage in the copying. The customer is better

⁴⁰ See Christopher D. Stone, *What to Do About Biodiversity: Property Rights, Public Goods, and the Earth's Biological Riches*, 68 S Cal L Rev 577, 580-81 nn 11-12 (1995) (discussing public-goods characteristics of nonrivalness and appropriability and comparing berry patches with private goods); Wendy J. Gordon, *Assertive Modesty: An Economics of Intangibles*, 94 Colum L Rev 2579, 2587-88 (1994) (explaining how public-good characteristics of intellectual property can lead to market failure); Wendy J. Gordon, *A Property Right in Self-Expression: Equality and Individualism in the Natural Law of Intellectual Property*, 102 Yale L J 1533 (1993) (comparing agricultural commodities and intellectual property and emphasizing public-goods characteristics of intellectual property).

⁴¹ The nonrival character of information means she can have her cake and eat it too.

off if she sells the copies for any amount of money greater than her cost of copying.

The nonrival character of digital information has two implications for our Web entrepreneur, both of them bad. First, the possibility of copying means that he is deprived of the sales made by his customer. Second, because his customer did not have to incur the costs of discovering the information and assembling the pointers, she can price them much more cheaply and still cover her costs—essentially, the mere cost of copying. Either the Web entrepreneur will not be able to sell anything because he maintains a higher price, sufficient to cover his higher costs; or, in order to compete effectively, he must price below his total cost, thus eventually driving himself out of business. This teaches the entrepreneurs a lesson—do not invest your energy in creating products like this because you will not be rewarded.

The foregoing parable explains the justification for the reproduction right in copyright law. In some respects this reproduction right seems similar to the traditional property interest that the farmer has in his tomato. Just as taking the farmer's tomato without his permission constitutes the tort of conversion, so also reproducing the Web entrepreneur's set of Web pointers without his permission may be copyright infringement.

There are, however, two difficulties with the analogy. First, unless the reproduction right is carefully limited, it may represent a significant barrier to the very activity it seeks to encourage.⁴² The consumer of the information product may need to reproduce the product to use it. Some reproduction of information products may be necessary to build other information products.

Second, a special reproduction right may not be necessary. A conventional property interest, sufficient to protect the farmer

⁴² Copyright seeks to encourage production of information value. See *Feist Publications, Inc. v Rural Telephone Service Co.*, 499 US 340, 349-350 (1991) (explaining justification for copyright). But copyright actually may have the effect of decreasing such production:

Although increased copyright protection may encourage the production of more copyrightable work, some of which might not otherwise be created, it also increases the price of intellectual works for consumers, and so reduces the dissemination and availability of such works. In some cases, those consumers may be producers of further works. Thus, the number of intellectual works in the community may be reduced and the speed at which the works are disseminated reduced. Limiting the defusion of expressions also limits the defusion of the ideas underlying those expressions.

Australian Economic Analysis of Copyright Report at 13 (cited in note 25).

against the theft of his tomato, also may be sufficient to protect the Web entrepreneur against the theft of the fruits of his labors. The exclusivity characteristic concerns means employed by a producer to exclude a consumer. A theater owner, for example, excludes consumers by showing his movie only within an enclosed theater and only admitting paying patrons. The movie is nonrival, but excludable. A recent study for the Australian government identified several features of publishing markets that could allow returns for a first publisher to remain high enough to cover the costs of producing the original, thus obviating the justification for intellectual property under the public-goods rationale.⁴³ These features include lead time, costly copying, less than perfect copies, inability to use copies without support and assistance from the originator, and collusion between potential copiers and originators.⁴⁴

Consider the efficacy of conventional property interests. The farmer benefits from these interests by fencing his tomato patch and asserting control over his stall in the marketplace. Anyone who takes tomatoes from the patch or the stall and sells them without the farmer's permission commits the torts of trespass to land,⁴⁵ trespass to chattel,⁴⁶ or conversion,⁴⁷ and the crimes of theft,⁴⁸ burglary,⁴⁹ or defiant trespass.⁵⁰ The rationale for these torts and crimes is the prevention of conduct inconsistent with the farmer's property interests in the tomatoes. Trespass, conversion, larceny, and burglary are applicable to information resources. If one fences off the information wares in one's computer, unauthorized entry may be remediable by property-oriented torts, such as trespass or conversion, and property-oriented crimes, such as burglary or larceny.⁵¹ Some new form of legal protection or property interest is necessary only when conventional property interests are insufficient. Historically, protecting against theft of the tangible object in which intellectual property was embodied, such as a book, protected the author and publish-

⁴³ Australian Economic Analysis of Copyright Report at 14 (cited in note 25).

⁴⁴ *Id.*

⁴⁵ Restatement (Second) of Torts § 158 (1965).

⁴⁶ *Id.* § 217.

⁴⁷ *Id.* § 222A.

⁴⁸ Model Penal Code § 223 (1985).

⁴⁹ *Id.* § 221.1.

⁵⁰ *Id.* § 221.2.

⁵¹ See Ga Code § 16-9-93 (1992) (defining computer theft); Iowa Code Ann § 716A.9 (1993) (defining computer theft); Minn Stat Ann § 609.89 (1987) (defining computer theft); RI Gen Laws § 11-52-4 (1994) (defining computer theft).

er to some degree, but did not protect them against the prospect that someone would copy the contents of the book and resell it. In the electronic context, it is important to identify the difference between theft of the tangible artifact and free riding on the intangible intellectual property. If technology makes it more difficult to steal the content of the "book" after buying or stealing the book, the gap to be filled by intellectual property, as opposed to conventional property, may be smaller.⁵²

Regardless of the respective roles that conventional and intellectual-property concepts play, all forms of property are limited by the needs of the larger society to do things that in some sense diminish the economic expectations of the property owner. For example, owners of real property never have enjoyed the privilege of engaging in conduct that constitutes a nuisance.⁵³ Early in the twentieth century, the common-law courts established that owners of real property do not enjoy the right to restrict flights over their property at reasonable altitudes.⁵⁴ More recently, environmental law has imposed further restrictions on property owners' rights and privileges.⁵⁵ Taking of private property, though entitling the property owner to compensation, similarly represents a limitation on uninhibited exploitation of private property. In all of these traditional examples, the law strikes a balance between the utility of private property and the utility of public use of what otherwise would be within the scope of private property.

The same balancing occurs in an intellectual-property regime. Absolute ownership of information potentially blocks use of the owned information. Since all information in some sense is derived from other information, ownership of information must be limited in order to avoid preemption of the information base from which public debate and various economic activities can take place.⁵⁶

⁵² Changes in technology also can change cost functions and change the relationship among fixed and variable costs and the importance of sunk costs, all of which affect free-ride potential, as explained in Part II of this Article.

⁵³ William Blackstone, 3 *Commentaries on the Laws of England* 216-19 (Callaghan & Co., 2d ed 1879) (summarizing cause of action for nuisance).

⁵⁴ See generally *San Diego Unified Port District v Superior Court*, 67 Cal App 3d 361, 136 Cal Rptr 557 (1977) (preempting trespass claims resulting from aircraft overflight).

⁵⁵ See *Lucas v South Carolina Coastal Council*, 505 US 1003, 1015 (1992) (recognizing proposition that environmental restrictions on property use could constitute a taking compensable under the Fifth and Fourteenth Amendments); *Penn Central Transportation Co. v New York City*, 438 US 104 (1978) (reviewing framework for analyzing regulatory-taking claims).

⁵⁶ *Feist*, 499 US at 349-350 (explaining why copyright must be limited); *Sony Corp. v*

II. ECONOMICS OF FREE RIDING

A. Coase's Caution

Professor Coase appropriately cautioned that policy judgments about his theorem and about transaction costs should be based on real-world facts, not on theory:

[H]ow is it that these great men have, in their economic writings, been led to make statements about lighthouses which are misleading as to the facts, whose meaning, if thought about in a concrete fashion, is quite unclear, and which, to the extent that they imply a policy conclusion, are very likely wrong? The explanation is that these references by economists to lighthouses are not the result of their having made a study of lighthouses or having read a detailed study by some other economist. Despite the extensive use of the lighthouse example in the literature, no economist, to my knowledge, has ever made a comprehensive study of lighthouse finance and administration.^[57] The lighthouse is sim-

Universal City Studios, Inc., 464 US 417, 431-32 (1984) (noting that limited scope of copyright reflects balance of competing claims on public interest; creative work must be encouraged but private motivation must ultimately serve cause of promoting broad public availability of information). See generally L. Ray Patterson and Stanley W. Lindberg, *The Nature of Copyright: A Law of Users' Rights* (University of Georgia Press, 1991) (arguing that copyright law should be interpreted to recognize users' rights as well as authors' rights).

⁵⁷ Professor Coase later suggested that perhaps the light from lighthouses is not a public good—at least on the excludability dimension:

The early history [of the British lighthouse system] shows that, contrary to the belief of many economists, a lighthouse service can be provided by private enterprise. In those days, shipowners and shippers could petition the Crown to allow a private individual to construct a lighthouse and to levy a (specified) toll on ships benefitting from it. The lighthouses were built, operated, financed and owned by private individuals, who could sell the lighthouse or dispose of it by bequest. The role of the government was limited the establishment and enforcement of property rights in the lighthouse. The charges were collected at the ports by agents for the lighthouses. The problem of enforcement was no different for them than for other suppliers of goods and services to the shipowner. The property rights were unusual only in that they stipulated the price that could be charged.

R. H. Coase, *The Lighthouse in Economics*, 17 J L & Econ 357, 375 (1974) (cited in note 38).

If a lighthouse owner knows when each ship needs the services of the lighthouse, and if only one ship is within range of the lighthouse at any moment, excludability is perfect because the light could be shut off when nonpaying ships come in range. *Id.* at 375-

ply plucked out of the air to serve as an illustration. The purpose of the lighthouse example is to provide "corroborative detail, intended to give artistic verisimilitude to an otherwise bald and unconvincing narrative."

This seems to me to be the wrong approach. I think we should try to develop generalisations which would give us guidance as to how various activities should best be organised and financed. But such generalisations are not likely to be helpful unless they are derived from studies of how such activities are actually carried out within different institutional frameworks. Such studies would enable us to discover which factors are important and which are not in determining the outcome and would lead to generalisations which have a solid base. They are also likely to serve another purpose, by showing us the richness of the social alternatives between which we can choose.⁵⁸

Professor Coase's caution is particularly appropriate when one thinks about new information technologies. The application of the Coase theorem to markets for information is debatable.⁵⁹ New information technologies may be misunderstood by policymakers and commentators. And, even if policymakers and commentators understand these technologies, the use of simplifying metaphors may obscure important realities. This Article argues that it is useful to begin with the actual transactions that occur in new cyberspace technologies. Those technological realities suggest that there may be important sources of excludability and rivalness for information products in the new environments that undercut any arguments in favor of expanding intellectual-property protection. As a recent report commissioned by the Australian government said, "[t]he . . . onus is on those advocating any expansion of copyright protection to show on a case-by-case basis that such extension would benefit producers and consumers."⁶⁰

76 n 43.

⁵⁸ Id at 374-75 (internal citation omitted).

⁵⁹ See Robert P. Merges, *Of Property Rules, Coase and Intellectual Property*, 94 Colum L Rev 2655, 2657-58 (1994) (noting difficulties in judging an argument over existence of externalities in intellectual-property field).

⁶⁰ Cover letter accompanying Australian Office of Regulation Review, and Economic Analysis of Copyright Reform (1995) (cited in note 25).

Of course, one must be careful not to build policy on transitory technology applications. For the foreseeable future, however, it is safe to assume that computers will be used to process information, that they will be connected in networks, that the networks will use open standards for their connections, and that the capabilities popularized through the Web will continue to be exploited. Thus, the Web model is not likely to become irrelevant any time in the near future.

Technology in the Web plays two important roles in analyzing the role of intellectual property. First, it reduces the nonexcludability and nonrivalness characteristics that justify intellectual-property protection. In this role, features of the technology that impose zero or only slight transaction costs between originator and initial consumer, while imposing very high transaction costs on potential free riders and pirates, reduce the overall transaction costs justifying intellectual property. Second, because the transaction costs resulting from the Web technology are asymmetric, they may not justify new configurations of property and liability entitlements in the evolution of intellectual property.

One justification for special property rules for information is the inability of the originator and initial owner of intellectual property to recover the cost of creation because of the potential of free riding.⁶¹ This argument suggests that, absent legal protection, the market will not produce enough information. Pirates do not have to repeat the investment of the creator, and thus can sell the creator's product at the marginal cost of copying, forcing the creator to price at the marginal cost of copying in order to retain any market share.⁶² At this price, the creator will never recover her fixed costs of creation.

Intellectual property law remedies this problem by increasing the pirate's costs.⁶³ Under a regime of intellectual property, the pirate faces not only the marginal cost of copying, but also

⁶¹ David H. Kramer, *Who Can Use Yesterday's News?: Video Monitoring and the Fair Use Doctrine*, 81 Georgetown L J 2345, 2360 (1993) (arguing that "socially desirable transfers between copyright holders and individuals . . . might not occur through the market" because of transaction costs and the free-rider problem).

⁶² *Id.*

⁶³ It may seem paradoxical that one reduces the transaction costs that justify intellectual-property law by increasing transaction costs to pirates. Two different kinds of transaction costs are involved. The first type is within the broad definition that encompasses impediments to negotiations, such as lack of excludability. The second type increases excludability and therefore decreases the first type of transaction cost by making it more difficult for a pirate to obtain and resell information without paying for it.

legal costs, which represent his expected liability.⁶⁴ A real pirate, moreover, faces additional costs. He must acquire the pirated information, transform it into a form that he can resell, and market it.

The costs of originator and pirate can be expressed in equation form. The originator's costs are:

$$C_o = C_c \ C_{ct} \ C_m \ C_r$$

where c_c is the cost of creation, for example, payments to the author; c_{ct} is the cost of chunking and tagging, or otherwise preparing the information for publication; c_m is the cost of marketing, including promotional expenses, distribution costs, and costs of billing and collection; and c_r is the cost of copying or reproduction.

The pirate's costs can be expressed as:

$$C_p = C_a \ C_t \ C_m \ C_r \ C_{ll}$$

where c_a is the cost of acquisition, for example, finding and downloading the material a pirate intends to resell; c_t is the cost of transformation;⁶⁵ c_m is the cost of marketing; c_r is the cost of copying; and c_{ll} is the pirate's cost of legal liability. There is no reason to expect that the pirate's marketing or copying costs will be lower than those of the originator.⁶⁶

A free-ride problem exists only if the pirate's costs are less than the originator's costs, in other words if

$$C_c \ C_{ct} > C_a \ C_t \ C_{ll}.$$

Professor Hardy's article,⁶⁷ the *White Paper*,⁶⁸ and other commentaries about property in cyberspace assume that $c_c \ C_{ct}$ is

⁶⁴ The expected liability in turn is a function of the probability of detection, the probability that a copyright owner could prove infringement, and the expected damages resulting from a judgment for the copyright owner.

⁶⁵ In conventional publishing, this would be the cost of typesetting and manufacturing.

⁶⁶ Indeed, the originator's learning curve and lead time probably will be such that her marketing and reproduction costs will be lower at any point in time than those of a pirate. But for the purpose of simplicity, this Article initially assumes that the marketing and copying costs are the same for both originator and pirate. When the effect of the originator's lead time is considered, the assumption is relaxed.

⁶⁷ Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U Chi Legal F 217 (cited in note 8).

⁶⁸ United States Department of Commerce, Information Infrastructure Task Force, *Intellectual Property and the National Information Infrastructure: Report of the Working Group on Intellectual Property Rights* (Sept 1995) ("White Paper") (cited in note 5).

much greater than c_a , c_t , and therefore that the value of c_{ii} must be increased to maintain the current level of free-riding risk.

This Article argues that that may not be so. In particular, it argues that products can be designed so as to increase c_t to the point where it counterbalances any reduction in c_{ii} that results from cyberspace technology. Product design can increase the benefits of the originator's lead time, thus increasing the probability of recovering fixed costs before the pirate can establish a market presence. Finally, the Article argues that payments can be transferred from those who gained from a relatively frictionless cyberspace⁶⁹ to creators who otherwise face free-riding risks.

When fixed investment is large compared with variable costs of production, free riding on the first producer's investment becomes a possibility. The imitator free rides by producing the same product at marginal costs close to those experienced by the innovator, but avoids the fixed costs incurred by the innovator.⁷⁰ It is not necessary that the free rider have no fixed costs; only that the free rider's fixed costs be less than the first producer,⁷¹ and that his marginal cost not be so much higher than the first producer's⁷² as to cancel the advantage of lower fixed costs. Accordingly, the free rider faces a lower average total cost and enjoys a price advantage over the innovator. The greater the free ride, the greater the cost advantage.

But there are countervailing considerations. The monopolies created by intellectual property may be unnecessary where significant economic barriers to entry exist.⁷³

⁶⁹ The frictionless condition refers to minimization of transaction costs otherwise associated with complex new schemes of intellectual-property protection or technological protection for creative works.

⁷⁰ In the conventional analysis of the economics of information, fixed costs usually means c_c —the originator's cost of creation—and the analysis ignores the pirate's fixed costs, c_a , c_t , and c_m .

⁷¹ It is also necessary that the first producer's fixed costs be sunk. Sunk costs are costs that the producer cannot recover by transferring to another through sale or lease. If the first producer has low fixed costs, relative to total costs, it becomes less likely that sunk costs are important. If fixed costs are relatively more important, the potential for important sunk-cost considerations increases.

⁷² As might occur because of the learning-curve effects of the originator's lead time.

⁷³ See C.C. von Weizacker, *A Welfare Analysis of Barriers to Entry*, 11 Bell J Econ 399 (1980). A barrier to entry is defined "as a cost of producing (at some or every rate of output) which must be borne by a firm which seeks to enter an industry but is not borne by firms already in the industry." Id at 399. See also Mark F. Grady and Jay I. Alexander, *Patent Law and Rent Dissipation*, 78 Va L Rev 305 (1992) (arguing that the purpose of patent law is to limit rent dissipation); Donald L. Martin, *Reducing Anticipated Rewards from Innovation through Patents: Or Less is More*, 78 Va L Rev 351 (1992) (com-

First, the potential free rider may not be able to avoid fixed costs to any great degree.⁷⁴ An example outside the information industry is the imitation of a new aircraft technology by another producer. The detailed engineering design and tooling required by the copier potentially overshadows the original producer's investment.⁷⁵ Second, there are delays before any copier can realize earnings from free riding.⁷⁶ Third, the first innovator gains reputational advantages, which assist in differentiating that producer's product from those of imitators. Fourth, the first innovator has a head start in taking advantage of learning-curve cost advantages which can deter entry and result in supranormal profits while the technology matures. Finally, firms already in a market use existing market structures to deter new entrants who lack production facilities, managerial experience, and channels of distribution.⁷⁷ In one survey, being first with an innovation, moving quickly down the learning curve, and having superior sales or service efforts exceeded patents as means of appropriating the benefits from innovation.⁷⁸ Similar barriers to successful entry can operate in the information industry.

In addition to the differences between fixed and variable costs, other barriers to entry by pirates may exist. Some fixed costs may represent transferable rather than sunk costs and thus

menting on Grady and Alexander article); Robert P. Merges, *Rent Control in the Patent District: Observations on the Grady-Alexander Thesis*, 78 Va L Rev 359 (1992) (commenting on Grady and Alexander article).

⁷⁴ Landes and Posner note that copiers may have positive fixed costs, though one would expect those fixed costs to be lower than those of the original publisher. William M. Landes and Richard A. Posner, *An Economic Analysis of Copyright Law*, 18 J Legal Stud 325, 329 (1989).

⁷⁵ Other surveys suggest that patents are very important in pharmaceuticals and other chemicals but less important in other industries, including "instruments." F.M. Scherer and David Ross, *Industrial Market Structure and Economic Performance* 629 (3d ed 1990). But see the "self regulating" argument in choreographic protection. One estimate, reported by Professor Scherer, suggests that research and development costs of duplicating major unpatented new products exceeds 50 percent of the original innovator's costs. *Id* at 627 (reporting work by Richard Levin et al, "appropriating the returns from industrial research and development," in *Brooking's Papers on Economic Activity* at 809 (no 3 1987)).

⁷⁶ Landes and Posner suggest that new technologies reduce the importance of this advantage because they reduce the cost of making copies and permit copies to be made more quickly. Landes & Posner, 18 J Legal Stud at 330 (cited in note 74).

⁷⁷ Scherer explains why monopolistic competition is a structure that produces more innovation faster than either pure monopoly or perfect competition, Scherer & Ross, *Industrial Market Structure and Economic Performance* at 630-42 (cited in note 75), and that much innovation occurs from small new entrants who apparently were able to move more quickly with fewer inhibitions resulting from existing market share. *Id* at 652-653.

⁷⁸ *Id* at 628 (citing and reporting results from Levin).

be less at risk. Publishers can reduce the incidence of sunk costs by automating certain publishing processes. Lower sunk costs reduce the amount of fixed investment available for free riding.

Fixed costs may be broken down into two separate components: sunk costs and transferable costs.⁷⁹ Sunk costs are product specific and the producer cannot recover them through sale or lease.⁸⁰ If an investment can be used for other purposes, it does not represent a sunk cost.⁸¹ Only the sunk portion of that investment is free rideable, because only it represents irreversible investments.⁸² Transferable costs, however, are not free rideable because the initial producer can sell the investment, recover its cost, and negate any cost advantage held by the free rider. Thus, free rideability depends on whether a significant part of a first producer's costs are sunk. Investment risk to an innovator decreases commensurately as it moves from irreversible to reversible investments⁸³—from sunk to transferable costs. A first producer will be much more willing to enter into a venture with lower investment risk represented by lower sunk investment. Labor, a major sunk cost, illustrates this point. Technological

⁷⁹ Traditional microeconomic analysis characterizes costs as fixed or variable, but for our purposes of determining free-ride potential, a sunk/transferable distinction is preferable.

⁸⁰ Professors Eaton and Lipsey illustrate sunk costs with two opposing illustrations. At one extreme is a natural monopolist who has no sunk costs. This might occur "if capital were not product specific and could be bought, sold, and rented on perfect markets." B. Curtis Eaton and Richard G. Lipsey, *Exit Barriers are Entry Barriers: the Durability of Capital as a Barrier to Entry*, 11 Bell J Econ 721, 722 (1980). Because there are no sunk costs, the market is contestable at each moment. At the other extreme is a natural monopolist with a "permanent commitment" to the market. Id. "[A]s long as he can cover his avoidable costs he will remain in the market." Id. See also B. Curtis Eaton and Richard G. Lipsey, *Capital, Commitment, and Entry Equilibrium*, 12 Bell J Econ 593, 594 (1981) (explaining that sunk costs are costs invested in product-specific capital determined in larger part by its durability and divisibility).

⁸¹ An example of a sunk cost is the cost charged to an online database subscriber for so many minutes of use of a particular Lexis or Westlaw database. Once a user's connect time has elapsed, the cost has been incurred. It is not recoverable through sale or lease since a subscriber has paid for a privilege that is no longer available. However, if a set of bound reporters are purchased instead, a transferable cost is incurred because the purchaser can readily resell the books.

⁸² Most of the literature on sunk cost focuses on economic incentives and disincentives for a firm considering entry into a market in which at least one other firm is operating successfully. For such potential new entrants, the risk is greater if the investment is irreversible. Building a railroad, for example, is riskier than starting an airline or a truck line because the cost of the right of way and track are sunk, while there is no equivalent investment in trucking or airlines.

⁸³ Although a free rider can appropriate the value generated by an initial producer's transferable costs, there is no free riding on the transferable cost because it can be sold. This results in no cost advantage to the free rider.

progress in electronic publishing has transformed labor-intensive activities into capital-intensive activities. The widespread use of computers in information production has made this apparent. When production is more labor-intensive, sunk costs are more likely because, once expended, labor cannot be used for another product.⁸⁴ However, as production becomes more capital-intensive, sunk costs become less likely because capital may be more easily sold or transferred for another use.⁸⁵ Accordingly, as information production—that is, electronic publishing—becomes more capital-intensive, transferable capital costs replace sunk labor costs. As these sunk costs decrease, free rideability decreases accordingly.⁸⁶

⁸⁴ For example, the cost representing the labor invested in creating the content for an information product is nonrecoverable. This cost is only recoverable by selling the information product. However, the transferability of the value created by the labor does not change its sunk-cost character. When discussing sunk costs, we look at transferability of inputs, not outputs. A sunk cost is a specialized investment having no value independent of the product in which it is embodied.

⁸⁵ Agriculture exemplifies a labor-intensive activity that has become increasingly capital-intensive. Agricultural machine technologies require less labor by intensifying use of capital, thereby decreasing agriculture's sunk costs because of the transferability of farm machinery.

Electronic publishing illustrates this same shift in the information-production industry. Activities involved in information production, such as chunking and tagging or creation of internal and external pointers, were at one time labor-intensive and represented sunk costs. However, its increased capital-intensity reduces these sunk costs. To illustrate, under older technologies, the labor expended in editing a manuscript represented a sunk cost. Using word-processing technology to automate this process makes it increasingly capital-intensive, and has reduced the producer's sunk costs. The investments in the necessary desktop computers and word-processing software represent transferable costs. While actual labor, a sunk cost, has decreased, the transferable costs involved in word processing have increased.

⁸⁶ Professor Breyer noted that increased technology actually increases a subsequent producer's cost advantage because the cost of copying decreases. Stephen Breyer, *The Uneasy Case for Copyright: A Study of Copyright in Books, Photocopies and Computer Programs*, 84 Harv L Rev 281, 298-299 (1970). While this may be true of products with high authorship value, it does not necessarily follow for those with low authorship value.

Certain information products rely exclusively on information in the public domain and have little to no authorship value. The human labor expended on content value represents a major sunk cost because of its nontransferability (assuming the absence of copyright protection). Accordingly, authorship value is dropped from consideration for these products, leaving only the labor and resources invested in the actual production as relevant economic considerations for free-ride potential. These costs are characterized as sunk and transferable costs as well.

A typical producer of an information product would have a cost function of:

$$C=f(c_s, c_t)$$

where c_s represents sunk costs and c_t represents transferable costs.

A producer of fiction novels, for example, faces this cost function. Using typical print-

B. How Traditional Electronic Publishing Tamed the Technological Risks to Intellectual Property

The introduction to this Article acknowledged that new information technologies disrupt historic balances between competing interests in intellectual property, but urged that appraisal of the disruptions focus on the specific free-riding and piracy risks created by the new technology. Acceptable balances among competing interests have been worked out reasonably well in electronic technologies used by proprietary, host-based electronic publishing systems. Before considering new challenges presented by open network environments like the Internet and its World Wide Web, one should consider how the balances have been struck in the more traditional electronic environments. This section considers the scope of legal protection for intellectual property, and the role of pricing, product design, bottlenecks, and enforceability, in the context of well-established, host-based, remotely accessible electronic publishing technologies.

Digital information technology emerged as a possible threat to intellectual property during the Second World War, when the first digital computer cracked the first enemy cipher or aimed the first bomb.⁸⁷ The technology reduced the cost of reproduction nearly to zero and facilitated incorporation of one work into another. These characteristics concerned the National Commission on New Technological Uses of Copyrighted Works ("CONTU")⁸⁸ and made the position of creators of digital works somewhat weaker than the position of creators of works on traditional media in terms of overall protection. These technological threats,

on-paper technology, a producer faces a relatively high amount of sunk costs because of the high amount of labor expended in adding content value, chunking and tagging value, external-pointers value, and so on. Accordingly, free-rider potential is high, resulting in the need for copyright protection. However, a producer of a product such as a publicly accessible database, Lexis for example, faces the same cost function, but enjoys a much lower sunk-cost investment. Technology allows this producer to expend little, if any, human labor in producing these same values. Free riding on this producer's investments is less likely than free riding on the print-on-paper producer's. Where technology decreases sunk costs, it may make copying—free riding—more difficult. It would seem, then, that new technologies affecting products with low authorship value, and a corresponding low sunk investment, would decrease free-ride potential. However, for products with high authorship value, and relatively higher sunk investment, technology may make copying easier, as noted by Professor Breyer. *Id.*

⁸⁷ See R. Moreau, *The Computer Comes of Age: the People, the Hardware, and the Software* (MIT Press, 1984).

⁸⁸ *Final Report of the National Commission on New Technological Uses of Copyrighted Works* 10 (National Commission on New Technological Uses of Copyrighted Works, 1978) (cited in note 3).

however, have been dealt with in pre-Internet environments through pricing and product design, as well as modest adaptation of intellectual property law, especially copyright law.

Although the case law is limited,⁸⁹ it is reasonably well accepted that a combination of copyright and contract protects the intellectual property of creators who sell information⁹⁰ on physical media like magnetic and optical disks, and through centralized host-based dial-up services such as CompuServe, America Online, Westlaw, and Lexis.⁹¹ In the market segment involving remote access—the one containing CompuServe, Lexis, and their competitors—the basic product relationships among content originator, electronic “retailer,” and customer are fairly well standardized, although pricing varies considerably. In the typical set of relationships, the content originator either transfers its copyright or grants an exclusive license to an enterprise that maintains the host computers and the dial-up communications facilities. For example, John Wiley & Sons, a conventional publisher, owns the copyright and grants a license for certain copyrighted works to West Publishing Company (“West”), in order to make the works accessible through Westlaw.⁹² West, in turn, acquires whatever copyright interests the publisher transferred to it under the license.⁹³ West also establishes contractual relationships with all of its customers, limiting what the customers can do with works accessed through Westlaw and obligating them to pay West according to its price schedule for access to Westlaw. West, under its contract with Wiley, pays a royalty. In this arrangement, West is the “retailer,” and Wiley is the “originator.”⁹⁴

⁸⁹ But see *West Publishing v Mead Data Central*, 799 F2d 1219 (8th Cir 1986).

⁹⁰ The intellectual-property problem is broader than protection for computer programs, the subject of the recent “manifesto” in the *Columbia Law Review*. Pamela Samuelson, et al, *A Manifesto Concerning the Legal Protection of Computer Programs*, 94 *Colum L Rev* 2308 (1994). Property in the information infrastructure includes not only computer programs—the procedures for handling information—but also the information content itself. Provisions of the Copyright Act explicitly aimed at computer programs, such as the archiving privilege, 17 USC § 117 (1994), do not explicitly extend to data such as messages or files involved in electronic communication and publishing.

⁹¹ But see *Beary v West Publishing Co.*, 763 F2d 66 (2d Cir 1985) (holding that West could not be sued for libel for publishing judicial opinion).

⁹² WESTLAW JW-EMPDIS.

⁹³ See generally *United States Naval Institute v Charter Communications, Inc.*, 936 F2d 692, 695 (2d Cir 1991) (explaining relationship between copyright infringement and breach of license); *Marshall v New Kids On the Block Partnership*, 780 F Supp 1005, 1008 (SD NY 1991) (same).

⁹⁴ Wiley is not actually the originator, but its ownership of the copyright puts it in the shoes of the originator.

Figure 1 illustrates the typical centralized-host electronic-publishing concept. The server not only provides pointers and other finding and retrieval value,⁹⁵ but it also publishes content.⁹⁶ The client deals only with the server, which looks like a conventional publisher. The host ensures payment for its intellectual property by denying a connection to those who have not paid or made payment arrangements.

A variety of common pricing arrangements exist.⁹⁷ For example, some works are available through Westlaw based on payment of the basic Westlaw fee, a combination of monthly and hourly charges. Access to other works results in a surcharge in addition to the basic Westlaw subscription fee. The royalty arrangements between originator and retailer also vary. For example, the retailer may keep track of the number of times a particular work is accessed,⁹⁸ and make royalty payments to the originator based on numbers of accesses, or it may simply obtain rights based on payment of a fixed fee for a license of a defined duration.

In current online electronic-publishing arrangements, the single bottleneck of the host-based retailer makes intellectual-property rights sufficiently enforceable to allow creative and entrepreneurial activity to flourish.⁹⁹ If a customer does not have a subscription relationship with Westlaw, the customer cannot obtain any information through the Westlaw service, because the first step in any dial-up connection is verification of an active account through an exchange of account name and password information with the host computer. The originator depends on this tollgate, defined in an express contract and enforced technologically, to protect its economic interest and to prevent piracy. The tollgate makes the information product excludable, thus weakening its public-goods character. The tollgate increases a pirate's c_a cost.

⁹⁵ See the rectangles in Figure 1.

⁹⁶ See the circle in Figure 1.

⁹⁷ See Henry H. Perritt, Jr., *How to Practice Law with Computers* 501-02 (Practising Law Institute, 2d ed 1992) (describing Westlaw and Lexis pricing structures).

⁹⁸ For example, America Online reportedly pays the originator 10-20 percent of the revenue it receives for particular content. Such an arrangement contemplates some mechanism for tracking the revenue attributable to particular content items, such as a pricing scheme that imposes a charge for access to that content.

⁹⁹ De Sola Pool suggests that this technological bottleneck always will be the natural focal point in intellectual-property regimes. Ithiel de Sola Pool, *Technologies of Freedom* 248-50 (Belknap Press, 1983).

To be sure, the nonrival nature of the digital format permits free riding and piracy by customers of the retailer. Once someone accesses a work through Westlaw, the accessor can duplicate the work and sell it in competition with Westlaw.¹⁰⁰ Such conduct, however, would not only violate the copyright interest of both originator and retailer, it also would violate the contract between the subscriber and the retailer. Moreover, the granularity¹⁰¹ of most works accessible through Westlaw and other host-based services makes it costly to download large amounts of content, as would be necessary for one wishing to engage in large-scale illegal redissemination.¹⁰² Fine granularity in remotely accessible databases may not only improve performance of the system for a consumer,¹⁰³ but it may also increase a pirate's costs to the point that piracy is unattractive.

The existence of a single tollgate makes violations of the copyright and license agreement relatively easy to prove. Records on access exist, and unobtrusive codes can easily be inserted in content to detect unauthorized copies.¹⁰⁴ The absence of much case law on license or copyright violations by subscribers to host-based services is consistent with an acceptable level of compliance with copyright and license terms. If widespread piracy existed, one would expect a greater incidence of civil and criminal enforcement actions.¹⁰⁵

¹⁰⁰ That is, the pirate's cost of transformation, c_t , is low.

¹⁰¹ Granularity in this context refers to the size of the information object that can be accessed with one command. Finely grained information resources would be available only a screen or paragraph at a time. Coarsely grained information resources would be available one document or file at a time. The usual granularity of Web resources is finer than resources available through file transfer protocol ("ftp").

¹⁰² Fine granularity increases the pirate's c_t . For example, this author's two volume work, Henry H. Perrit, *Employee Dismissal Law and Practice*, (Wiley Law Publications, 2d ed 1987), is available on Westlaw, but a user does not get access to the entire two-volume work with one request. Rather, each of approximately 250 sections of the work constitutes a separate Westlaw "document." A pirate wishing to use Westlaw access as the starting point for illegal redissemination of the entire work would have to download all 250 sections independently. This task would not be impossible, but it would be cumbersome and therefore costly.

¹⁰³ Fine granularity increases performance for consumers by allowing the consumer to view a piece of information more quickly, rather than waiting for a larger quantity of information, such as the entire document, to be downloaded before viewing is permitted.

¹⁰⁴ This increases the pirate's c_{11} .

¹⁰⁵ But see *West Publishing Co. v On Point Solutions, Inc.*, 1994 US Dist Lexis 20040 (ND Ga, Sept 1, 1994) (enforcing West's copyright in the editorial enhancements it adds to cases).

C. Why Internet-Like Architectures Threaten Intellectual Property

The Internet is a model of an open network architecture that will likely dominate electronic publishing in the future. The transaction costs and the resulting possibilities for excludability and rivalness are significantly different from those of host-based architectures.

The Internet is an international network of computers and computer networks connected to each other through routers using the TCP/IP protocols and sharing a common name and address space. One can communicate with any computer connected to the Internet simply by establishing a connection to an Internet router or node. The Internet is not a corporation or administrative arrangement; it is a method for connecting computer systems. Voluntary cooperative bodies, such as the Internet Engineering Task Force ("IETF"), discuss and formulate standards and protocols through documents called requests for comments ("RFCs"). The Internet began in the 1960s with federally subsidized connections among universities and government research laboratories. An "acceptable use policy" limited traffic unrelated to research and education. By 1990, the Internet's potential as a model for a National Information Infrastructure ("NII") had been recognized. The federal government began to reduce the subsidy and to encourage private entities to take over responsibility for basic communication and traffic management functions. By 1995, most of the traffic on the Internet involved unsubsidized facilities and private traffic. The Internet is the archetypical open network.

Widely used Internet applications (in addition to e-mail) include *telnet*, a method of establishing a remote terminal connection to another computer across the Internet; *file transfer protocol* ("ftp"), a means for transferring files between computers linked together by the Internet; *gopher*, a user-friendly menuing system for making files and text available (now largely replaced by the World Wide Web); *news* and *newsgroups*, means for electronic discussions in which anyone connected to an Internet node has access to posted messages and replies to them; and the *World Wide Web*.

The World Wide Web ("Web") is a particularly popular application for the Internet. Reflecting the client-server model of computer-program design,¹⁰⁶ the Web makes use of two kinds of

¹⁰⁶ While general purpose computers can be classified in many ways, a useful distinc-

software: server software and client or "browser" software. The client and the server work together during a Web session, communicating with each other through messages and files conforming to the hypertext transfer protocol ("http")¹⁰⁷ and hypertext markup language ("html") standards.¹⁰⁸ Documents formatted in html are displayed by browser software that presents colors, typeface styles and sizes, and hypertext links as highlighted text, all according to html instructions or tags.

An increasingly popular form of electronic publishing involves taking documents, graphical images, sound files, or a combination of these, and placing them on a Web server—usually a small or medium-sized Internet server with several directories devoted to Web files and the server application software. The Web is a *hypertext* system, meaning that a typical Web document has pointers to other html documents. These other documents may be located anywhere in the Internet—on a Web server, on the same server on which the pointer is located, or on other parts of the same document that contains the pointer.

For example, one could take this Article and organize it for electronic publishing on a Web server by substituting internal hypertext pointers for all of the cross references and by substituting external hypertext pointers for all of the reference information in the footnotes. When a Web browser displays the document, each of the pointers, internal or external, would appear as highlighted text or as a small symbol. A user interested in the highlighted information would click on the highlighted text with

tion for purposes of this Article distinguishes *servers* from *clients*. Servers store and process information for a multiplicity of clients. Servers are usually more powerful than clients and range in size from slightly souped-up desktop computers using 386, 486, or Pentium chips, to clusters of the largest mainframe computers. Client computers conceptually can be of any size, but in most configurations familiar to practicing lawyers, the client computer is the computer with which a human being directly interacts—for example, a notebook or desktop computer. In a typical Lexis session, the computer on the lawyer's desktop or the terminal in the library is the client, and the array of mainframe computers in Dayton is the server.

In the client/server model of computer-system design, functions can be allocated between server and client to optimize performance. For example, in both the Westlaw and Lexis systems, the client manages the graphical user interface, presenting the appropriate icons and text on the screen, while the server maintains the data and responds to user requests for particular statutes or cases. Henry H. Perritt, Jr., *Law and the Information Superhighway* § 1.2 (John Wiley & Sons, 1996).

¹⁰⁷ Http is the protocol that defines how Web servers exchange information with, and respond to, requests from Web clients.

¹⁰⁸ Html is the protocol for tagging certain parts of a document published on the Web so that they show up in particular typefaces or styles, or so that they can be used as pointers to other information objects on the same or other local servers.

his mouse. This would cause the Web to retrieve the identified information and to automatically display it on the client screen.

Thus, the Web organizes information distributed across the Internet. It facilitates unbundling because editors or publishers interested in collecting resources related to a particular subject need not obtain or maintain actual copies of the content of the resources; they can make their knowledge available simply by writing a Web document that contains pointers to the identified references and information about the significance of the resources. The clearest example is a typical law review footnote or citation in a legal brief. One can make the cited case or statute available simply by pointing to it in the law review article or brief. A user reading the law review article or brief can retrieve the full text pointed to simply by clicking on the footnote or citation.

Figure 2 illustrates how the Internet and similar architectures permit value-added products to be unbundled, with different elements of the bundle being supplied by different entities. The bundling of these elements occurs according to the desires of a particular user at the time the user wants the complete value-added information product. In this architecture, suppliers of information content¹⁰⁹ supply their content to anyone who wants it simply by putting files on computers connected to the Internet, called servers or "content servers."

Those value-added features are supplied by others.¹¹⁰ It is entirely possible with Internet applications like the Web for an entity to supply only index or table of contents-type value in the form of pointers to content. The pointers are implemented through Web pages and lists or Gopher menus on an Internet server that offers no other kinds of value. Someone else can provide user-friendly interface software through another server. Yet another person can provide connection services that permit connections through dial-up telephone lines or through higher speed dedicated links.

When a user wishes to identify and obtain a particular type of content, the user interacts with several Internet servers operated by different entities. First, the user establishes a connection to the Internet through a connection-services provider. The user then establishes a connection to an index provider. From the

¹⁰⁹ See the circles above the solid line in Figure 2. As Figure 2 indicates, content suppliers may be governmental entities, as for statutes and judicial opinions, or private-sector entities.

¹¹⁰ See the rectangles below the solid line in Figure 2.

lists, tables, and menus provided by the index server, the user identifies one or more items of interest. The index server uploads the pointers (not the content, because the index server does not have the content) through the Internet to the user's client computer. Then the user's client computer executes the pointers, which automatically downloads the identified content from the content server into the client computer.¹¹¹

This is a kind of assembly line for pieces of information value. It produces the product just in time, rather than producing it in bulk according to someone else's design. It lets the user design the product on an ad hoc basis.

Such an infrastructure is not only two layered; in many cases a pointer points, not directly to the full information resource, but to another collection of pointers, which may point to still other collections of pointers, and so on, collectively marking a trail to the complete resource. The computer programs involved assemble a trail from the three pointers and then retrieve the desired content from wherever it resides, directly into the computer of the requester, without the content having to traverse all the intermediary computers. Whether an intermediary points directly or indirectly to the desired resource is inherently an engineering decision driven by performance considerations. In many cases, the computer automatically decides to maintain copies of a particular information resource without any human intervention. A clear example of this is the caching of recently retrieved resources within a Web browser, such as Netscape.

Figure 3 illustrates a typical set of relationships among Web servers. Web server X (the consumer's intermediary) never possesses the content. It points to server Y (the pure intermediary), which in turn points to server Z (the originator's intermediary). Z, in turn, points to the content on the originator's server.¹¹² Transactions 1-6 with servers X, Y, and Z are requests for, and transmissions of, pointers only. The eventual request for, and

¹¹¹ To extend the example of publishing this Article on the Web, the *University of Chicago Legal Forum* would maintain a Web server (or a page on a Web server) containing pointers to the articles making up this volume. The text of the articles would be maintained on other computers running Web servers, this author's at Villanova (<http://www.law.vill.edu>), Professor Hardy's at William & Mary, Professor Post's at Georgetown, and so on.

¹¹² In some of the discussions below, the infringer is in the position of the originator, and one can understand the ultimate retrieval of content as referring to retrieval of infringing material.

retrieval of, the content transpires entirely between the client and the content originator, in 7 and 8.¹¹³

One must ask two sets of questions. First, what features of the technology increase excludability and/or rivalness and thus reduce the need for legal grants of entitlements to stimulate allocative efficiency? Second, how should one describe the transaction costs confronting various participants in the Web and draw conclusions about property versus liability-based entitlements and the identity of beneficiaries? This Article addresses the first question below and discusses different forms of protection for content. It addresses the second question in Part III and discusses intermediary liability.

One of the core concepts of the Internet and other open architectures is that information storage and processing functions are distributed rather than being centralized in a single host. Another core concept is the absence of proprietary protocols or technologies that isolate relationships among particular originators, retailers, and customers. Instead of an originator like Wiley having a single, exclusive relationship with one retailer like West as in the preceding example, an originator on the Internet is expected to have a multiplicity of relationships with several retailers. The open and distributed characteristics greatly weaken the techniques developed in host-based structures for protection of intellectual property.

The Web is the best example of how a content originator is threatened. But the Web is also the best example of the potential of Internet-like architectures for new forms of electronic publishing. In the Web, a content originator publishes his work simply by placing a file containing the content on an Internet Web server and allowing access to that server and file through the standard Web protocols, http and html. Anyone who wishes to view or otherwise use that content can do so simply by establishing a connection to the originator's server and pointing to that file

¹¹³ If the content on the originator's server is infringing, the Web server that simply points to other content servers is rather like someone who gives directions to the dirty-movie studio or the drug dealer. While the supplier of the pointers can be said to be involved in the distribution chain, the operator never comes in contact with the accused material. Certainly, in the copyright setting, this eliminates *prima facie* liability because the server has not engaged in any of the acts reserved exclusively to the copyright owner. On the other hand, there is the possibility of vicarious liability under other theories.

with a standard pointer in the URL format.¹¹⁴ A potential pirate's c_a is low.

Because search costs would be too great for potential users of information published in this fashion to know about all potential sources, the Web depends on a variety of more or less independent intermediaries who add value to the system by supplying pointers. In other words, someone wishing to access information from law reviews typically starts with an Internet node known for identifying legal resources on the Internet¹¹⁵ and finds on such a service a pointer to a particular law review file on another Internet node. Frequently, a user goes through two or more such intermediaries, perhaps beginning with one identifying a broad range of legal resources, which points to a particular law school, which in turn, points to a particular law review issue and article.

The breadth of the market reachable by the content originator depends upon a large number of intermediaries pointing to its works. This is good, for the content originator. His revenue potential is much greater than if he were limited to the market reached by a single distributor.¹¹⁶ Usually, the content publishers do not have prior arrangements with the pointer intermediaries; indeed, ordinarily they do not even know about and cannot limit who points to their works.¹¹⁷ This is bad for the content originator. He cannot make contractual arrangements for royalties or fixed-fee licenses with retailers he does not know. In other words, the transaction costs of effective licensing are high.

This does not change copyright law, and thus does not change the copyright protection for the content originator, except insofar as placement of its work on a Web server impliedly licenses certain uses¹¹⁸ or, less likely, places the work in the pub-

¹¹⁴ An example of a URL is "http://www.law.vill.edu/perritt/ombreport." This points to a particular computer connected to the Internet (www.law.vill.edu) and further identifies a particular file on that computer (OMB Report in the subdirectory perritt).

¹¹⁵ For example, http://www.law.vill.edu.

¹¹⁶ See Steve Lohr, *On-Line Stars Hear Siren Call of Free Agency*, NY Times 37 (Nov 25, 1995) (reporting on growing tendency of content originators, including discussion-group organizers, to move away from exclusive arrangements with CompuServe and America Online into nonexclusive distribution through Internet).

¹¹⁷ One can limit access to particular material on an Internet Web server, however, by requiring a password to access certain directories and files.

¹¹⁸ The *White Paper* described the implied-license analysis in the following way:

A nonexclusive license may be implied from conduct. Implied licenses, like oral licenses, are always nonexclusive in nature and may be limited in scope. Delivery of a copy of a work by the copyright owner to the moderator of a newsgroup may imply a license to reproduce and distribute copies of the work to the sub-

lic domain.¹¹⁹ Effective contract protection for the content originator, however, is more problematic.¹²⁰ While the content originator can post various terms and conditions in its work, or can post various messages on its Web server, there is no assurance that an intermediary or an end user will see any of these limitations until it actually accesses the content.

Intermediaries are even less likely than end users to be bound by posted limitations on use. The intermediary may be entirely unaware of such posted terms of conditions, never seeing the content to which it points.¹²¹ The likelihood is somewhat greater that the end users might be bound by terms and conditions because end users are more likely to read the contents at some point, and thus become aware of terms and conditions bound to the content. But even if end users are bound, they are far less satisfactory defendants, from the originator's perspective, than intermediaries, as in conventional host-based arrangements. In other words, the bottleneck that is the heart of intellectual-property protection and host-based networks does not exist naturally in open network architectures.¹²²

scribers of that newsgroup, but may not be evidence of an implied license to reproduce and distribute copies to other newsgroups.

White Paper at 116-17 n 424 (internal citations omitted) (cited in note 5).

¹¹⁹ Copyright owners may relinquish their property interest and put their works in the public domain. *Sanga Music, Inc. v EMI Blackwood Music, Inc.*, 55 F3d 756, 759-61 (2d Cir 1995) (holding that owner of common-law copyright in song placed song in public domain by teaching it to folk singer without communicating any restrictions except the hope that he would keep the song alive; applying 1909 statute, Copyright Act of 1909, 35 Stat 1075, codified as amended in 17 USC §§ 1-65 (1940)); *White Paper* at 15 (cited in note 5). Under the 1909 Act, it was easier to reach a public-domain conclusion because the author of a work established or maintained a statutory copyright only by complying with certain formalities, such as including a copyright notice on any published versions of the work. *Sanga Music*, 55 F2d at 759-60 (describing formalities and relationship to 1909 Act).

¹²⁰ Saying that contract protection is problematic is another way of saying that the transaction costs of effective negotiation are high.

¹²¹ Limitations do not bind a person accepting an offer unless they are communicated to the accepting party in a means likely to give the accepting party actual notice of the limitations. Restatement (Second) of Contracts § 39 (1981). See also *American Computer Trust Leasing v Jack Farrell Implement Co.*, 763 F Supp 1473, 1488 (D Minn 1991) (holding that disclaimers of warranty must be conspicuous). Disclaimers of warranties are analogous to limitations on the use of intellectual property because both negate rights or privileges that otherwise may accrue to the transferee of the property. Nevertheless, B may accept A's offer without subjective intent by B. See generally Restatement (Second) of Contracts § 23 (1981) and accompanying illustrations. Posted terms and conditions on automatically accessed works are thus the ultimate shrink-wrap license agreement.

¹²² *White Paper* § I.8.d at 103-11 (cited in note 5) (marshalling arguments against special immunities against copyright infringement for intermediaries in NII). The authors

Moreover, contract protection is unavailable except when privity of contract exists. Thus, the originator's contract position is even weaker with respect to pirates who get access not directly from the originator, but through others, such as intermediaries several steps removed. Privity requires either specialized communications, through, for example, Electronic Data Interchange ("EDI") transaction sets, that satisfy requirements for contractual offer and acceptance without human involvement or contemporaneous human assent to contract terms.

The possibility exists, of course, of refusing intermediary connections unless prior arrangements have been made with that particular intermediary. The Internet and Web offer the possibility of allowing access to particular files or directories only to preauthorized users who give the correct password.¹²³ The exchange of user-authorization information can be automated to establish a kind of trusted intermediary network. This technology permits electronic publishing through the Internet to rely on the same user account and password protections as host-based services. The possibility of transforming the Internet-like architectures into something close to host-based architectures, however, is not a fully satisfactory answer. It vitiates many of the advantages of an open architecture for new kinds of publishing and blocks the flow of information, the goal of intellectual property. The transaction costs of making prior arrangements are significant, and a content originator shrinks his market considerably by allowing access only through such prearranged intermediaries.

III. INTERMEDIARY LIABILITY AS A COUNTERVAILING PROBLEM

At the same time that open architectures may make it more difficult for content originators to protect their intellectual property, open architectures also may increase the exposure of intermediaries to liability for intellectual-property infringement.

In the Web, multiple intermediaries may interact to allow a consumer to retrieve information directly from a content originator.¹²⁴ An information object allegedly infringing another's

of the *White Paper* assert that the intermediary may be in a much better position to police compliance with intellectual-property law than owners of the intellectual property. *Id.* § I.8.d at 105-06.

¹²³ See, for example, <http://www.law.vill.edu:2000> (granting limited access to certain electronic discussion groups).

¹²⁴ A Web server typically presents a user with highlighted "hyper-media links" on menu items representing full-content text, images, sound, or video files. A user retrieves the indicated item simply by selecting the menu item or highlighted hyper-media pointer.

copyright may move through several intermediaries in this distribution system. The potential liability of the various intermediaries for copyright infringement is a matter of obvious interest both to the intermediaries and to the copyright owner alleging infringement. The copyright owner may perceive the intermediaries as having deeper pockets, or as being more amenable to personal jurisdiction than the originator of the allegedly infringing object.¹²⁵ Targeting the intermediary for a copyright infringement action is natural, considering the traditional role of the intermediary as a bottleneck on which intellectual-property protection focuses.

It may be relatively easy for the person claiming infringement to establish a violation of one of the exclusive section 106 rights¹²⁶ by the originator of the allegedly infringing item. The originator (pirate) almost certainly has reproduced the copyrighted work and also probably helped to distribute it to the public.¹²⁷ It is somewhat less clear whether the intermediaries have infringed any section 106 rights; this depends on the network architecture.

Intermediary liability is more likely in traditional bulletin-board arrangements¹²⁸ than in the Web. Consider the case of a dial-up electronic bulletin board, where any item selected and

This causes the server displaying the pointer to download a short computer-executable pointer, called a URL, to the user's computer. The user's computer, running Web client software, then automatically executes the URL to retrieve the information directly from the computer pointed to by the URL. The first computer that supplied the URL disconnects as soon as it has transmitted the URL to the user. Thus, although it appears to the user that the first computer retrieves the information item, in fact, another computer retrieves it. The Web process is commonly replicated through a chain of intermediaries, the first Web server pointing to another, and the second pointing to a third, and so on, with each intermediary server simply sending URLs to the customer. This occurs until the full content of the desired item is finally retrieved. Throughout the chain, a typical user perceives that everything comes from the first Web-server computer.

¹²⁵ Another kind of intermediary liability is attractive to originators: contract-based liability premised on the intermediary facilitating unwanted distribution of the originator's work. In this case, it is the access to original work that constitutes the wrongful conduct. In the case described in the text, it is access to an infringing work.

¹²⁶ 17 USC § 106 (1994) (enumerating rights exclusively belonging to a copyright owner).

¹²⁷ This violates the reproduction right, 17 USC § 106(1), and the distribution right, 17 USC § 106(3).

¹²⁸ Traditional commercial host-based information services, considered in Part III of this Article, are unlikely to face liability for intellectual-property infringement because they acquire rights to the content which they make available. Bulletin-board operators, on the other hand, are more likely to serve as conduits for persons who upload files for use by others. The uploaded files may be infringing, unbeknownst to the bulletin-board operator.

retrieved actually resides in the form of a file on the intermediary computer.¹²⁹ When the user selects a file, including an infringing one, the intermediary computer makes a copy and downloads it to the user's computer. When the intermediary makes the copy, it violates the section 106 reproduction right; when the intermediary downloads, it may violate the section 106 distribution right if it is aimed at the "public." The owner of the bulletin board may argue that it did not place the allegedly infringing item on its computer and did not itself cause the copy to be made. Rather, one copy was made by the third person placing the item on the bulletin board, and another by the user retrieving it. Such arguments failed in *Playboy Enterprises, Inc. v Frena*,¹³⁰ where the district court found that the operator of the electronic bulletin board on which third parties placed digitized images of Playboy centerfolds infringed Playboy's distribution rights as the content originator.¹³¹ Moreover, such a bulletin-board operator may have publicly performed or displayed the work¹³² when a user browsed material on the bulletin board.¹³³

¹²⁹ In other words, the computer ultimately transmitting the full-content item is the same computer that generates the interface made available to the requesting user.

¹³⁰ 839 F Supp 1552, 1556 (MD Fla 1993).

¹³¹ See *Sega Enterprise, Ltd. v MAPHIA*, 857 F Supp 679, 686 (ND Cal 1994) (finding that uploading of copyrighted material by third party to bulletin board constituted the making of unauthorized copies attributable to the bulletin-board operator). In *Religious Technology Center v Netcom On-Line Communication Services, Inc.*, 907 F Supp 1361 (ND Cal 1995), a district court held that a news server was not liable for direct copyright infringement because the copying that occurred in its system was triggered by the acts of a third party, placing the defendant in a position analogous to the operator of a copy machine, who makes available a process that makes copies under the direction of another. The court characterized the question as "whether processors of computers are liable for incidental copies automatically made on their computers using their software as part of a process initiated by a third party." *Id* at 1368.

The court gave the following answer:

The court believes that Netcom's act of designing or implementing a system that automatically and uniformly creates temporary copies of all data sent through it is not unlike that of the owner of a copying machine who lets the public make copies with it. [footnote omitted] Although some of the people using the machine may directly infringe copyrights, courts analyze the machine owner's liability under the rubric of contributory infringement, not direct infringement.

Id at 1369.

On the other hand, the court found the plaintiff entitled to trial on its allegations of contributory infringement and vicarious liability, based on the notice of infringement given by the copyright owner and the fact that the defendant received revenue from the accused activity. *Id* at 1373-77.

¹³² Public performance and display are, along with reproduction and distribution, rights that belong exclusively to the copyright holder. 17 USC § 106 (1994).

¹³³ See United States Department of Commerce, Information Infrastructure Task

Intent is irrelevant when conduct falling within section 106 occurs. *Playboy Enterprises* held that “[i]t does not matter that [a defendant] may have been unaware of the copyright infringement. Intent to infringe is not needed to find copyright infringement.”¹³⁴ In other words, intermediaries are subject to no-fault liability.¹³⁵

Technology matters. The infringement case against intermediaries who provide anonymous ftp sites is essentially the same as the case against electronic bulletin-board operators. On the other hand, the case against Gopher and Web servers is more tenuous. They never have possession of a requested item, which makes it less plausible that they have reproduced, distributed, displayed, or performed it.¹³⁶ Rather, they are more like providers of bibliographies to works, some of which may be infringing.

Nevertheless, copyright owners may argue that the scope of the section 106 duties should be extended to intermediaries as well, because they constitute links in a chain that necessarily results in the conduct covered by section 106. Copyright infringement is a statutory tort. The causation requirement in tort law long has been satisfied by the doing of an act intended to and substantially certain to result in the injury constituting the tort.¹³⁷

Moreover, even if Gopher and Web-type services do not expose their providers to liability for direct infringement, as in *Playboy Enterprises*, they may expose their providers to liability

Force, *Intellectual Property and the National Information Infrastructure: Report of the Working Group on Intellectual Property Rights* §§ I(A)(6)(d) at 63-64 nn 221-222 (Sept 1995) (“White Paper”) (cited in note 5) (noting that mere file transfer would not constitute performance, but suggesting that browsing of digitized Playboy images or other works would constitute a public display). The *White Paper* notes that “many NII uses would appear to fall within the law’s current comprehension of ‘public display.’” *Id.* § I(A)(6)(e) at 65, citing *Columbia Pictures Industries, Inc. v. Redd Horne, Inc.*, 749 F.2d 154 (3d Cir 1984) (holding video-store operator liable for public performance for renting tapes to customers who viewed them in semiprivate screening rooms) as authority for proposition that public-performance concept keeps pace with new technologies for allowing multiple persons to view stored material.

¹³⁴ *Playboy Enterprises*, 839 F Supp at 1559 (finding infringement based both on distribution and display rights).

¹³⁵ See also *MAPHIA*, 857 F Supp at 686-87 (holding that even if defendants did not know exactly when games would be uploaded, they provided facilities, direction, and encouragement, and thus were liable for contributory infringement).

¹³⁶ When Web servers cache material, they do reproduce content, and thus may face greater exposure. See Part V.

¹³⁷ See *Rose v. Isenhour Brick & Tile Co.*, 461 SE2d 782, 784 (NC App 1995) (engaging in conduct “knowing it is substantially certain to cause serious injury” constitutes a tort (emphasis in original)).

for derivative or contributory infringement.¹³⁸ In *Sony Corporation of America v Universal City Studios, Inc.*,¹³⁹ the leading case on contributory infringement, the Supreme Court held that manufacturers of video cassette recorders were not liable for contributory infringement of televised works recorded on their machines by consumers.¹⁴⁰ The Court held that systems capable of substantial noninfringing uses cannot produce contributory infringement.¹⁴¹ In order to apply this test to the Gopher or Web server, one must ask whether the particular server facilitates access to noninfringing information objects. If its purpose is not infringing, the fact that consumers may occasionally use the server to retrieve infringing objects does not suffice to establish contributory infringement by the operator of the server. On the other hand, if the server has the predominant purpose of facilitating access to infringing objects, the operator of the server should be liable for contributory infringement.

The *White Paper* apparently envisions a more extensive role for contributory liability. In regard to intermediary liability, the *White Paper* states:

There is a view that on-line service providers, such as bulletin board operators, should be exempt from liability or given a higher standard for liability, such as imposing liability only in those cases where infringement was willful and repeated or where it was proven that the service provider had both "actual knowledge" of the infringing activity and the "ability and authority" to terminate such activity. The latter proposed standard would combine the contributory infringement standard with the requirements for vicarious liability and apply it to all infringements (including direct infringements) of the service provider. Altering the standards of liability for infringement would be a significant departure from current copyright principles and law and would

¹³⁸ See *Netcom*, 907 F Supp at 1373-75 (allowing trial on contributory-infringement claim).

¹³⁹ 464 US 417 (1984) (5-4 decision).

¹⁴⁰ The Court constructed a two-tiered analysis. First, the Court found that the consumer conduct fell within the fair-use definition, and therefore did not constitute infringement at all. Second, the Court held that if the ultimate use of the system was noninfringing, then there could be no vicarious liability. The second part of the analysis is of more immediate importance to assessing the possibility of contributory liability by intermediaries. *Sony Corporation*, 464 US at 421.

¹⁴¹ *Id* at 440.

result in a substantial derogation of the rights of copy-right owners. It is a difficult issue, with colorable arguments on each side.¹⁴²

While acknowledging that it is virtually impossible for intermediaries to review messages and files for infringement possibilities contemporaneously, the *White Paper* also identifies other actors in the larger information infrastructure confronted with the same impossibility of screening. These actors include photo finishers, booksellers, record stores, newsstands, and computer-software retailers, all of whom nevertheless are subject to strict liability for infringement.¹⁴³ The *White Paper* also states that "on-line service providers can certainly investigate and take appropriate action when notified of the existence of infringing material on their systems and thus limit their liability for damages to those for infringement."¹⁴⁴ This has been part of the business costs for many other information distributors, and the authors of the *White Paper* saw no reason that NII intermediaries should be placed in a more favorable position.¹⁴⁵

The *White Paper* then focuses on a subclass of intermediaries. "On-line service providers have a business relationship with their subscribers. They—and, perhaps, only they—are in the position to know the identity and activities of their subscribers and to stop unlawful activities."¹⁴⁶ This, of course, is not true of many Web servers. The *White Paper* acknowledges that "[n]o one rule may be appropriate."¹⁴⁷ For example, an entity providing:

Only the wires and conduits—such as the telephone company . . . would have a good argument for an exemption if it was truly in the same position as a common carrier and could not control who or what was on its system. The same could be true for an on-line service provider who unknowingly transmitted encrypted infringing material.¹⁴⁸

The *White Paper* states that Congress believes that the limitation on damages for innocent infringers is adequate to protect inter-

¹⁴² *White Paper* at 103 (cited in note 5).

¹⁴³ *Id.* at 104.

¹⁴⁴ *Id.* at 105.

¹⁴⁵ *Id.*

¹⁴⁶ *White Paper* at 105 (cited in note 5).

¹⁴⁷ *Id.* at 110.

¹⁴⁸ *Id.*

mediaries while sufficient to create incentives for intermediaries to work with copyright owners and their subscribers to protect against infringement.¹⁴⁹

The *White Paper* reviews various forms of vicarious liability as a basis for holding intermediaries liable. The dance-hall cases justify holding liable any intermediary who authorizes infringing uses of his facility, such as the sponsor of an anonymous ftp server or electronic bulletin-board design for uploading infringing material.¹⁵⁰ More broadly, the *White Paper* suggests that an intermediary who provides services or equipment relating to the direct infringement may be liable for contributory infringement.¹⁵¹ It also suggests that "infringement liability may be based on the provision of equipment or other instrumentalities or goods used in or related to the infringement,"¹⁵² acknowledging *Sony*.¹⁵³ One could interpret the *White Paper* as arguing for a very broad regime of contributory infringement that might conceivably even sweep up Web and Gopher intermediaries who never engage in reproduction or direct distribution of copies.

Even under a more traditional application of infringement concepts, Web intermediaries might be liable for making and distributing copies because they use caching. Caching refers to the automatic copying of material to improve performance of computer systems. It is used in wide-area networks like the Internet to reduce the time required for second and subsequent access to Web files. Because caching involves copying, it raises particular concerns about potential copyright violations.

This Article presumes that the supplier of information content has made it available on the Web through a "content server" ("CS"), a Web server from which the content may be retrieved. The Article further assumes that this content supplier has imposed restrictions on the content thus published, permitting access for purposes of browsing and viewing, but not copying.¹⁵⁴

Caching may constitute prima facie direct copyright infringement.¹⁵⁵ Suppose that there are three entities, besides the con-

¹⁴⁹ Id at 107-08.

¹⁵⁰ *White Paper* at 99 (describing dance-hall case concept) (cited in note 5).

¹⁵¹ Id at 100.

¹⁵² Id.

¹⁵³ Id. The *White Paper* cites *Cable/Home Communication Corp. v Network Products, Inc.*, 902 F2d 829, 845-47 (11th Cir 1990), in support of its conclusion that providing facilities can result in contributory infringement. *White Paper* at 100 (cited in note 5).

¹⁵⁴ The content supplier might be tempted to permit viewing and browsing, but not "downloading." The difficulty with this distinction is that downloading is necessary to permit browsing and viewing on the client computer.

¹⁵⁵ The approach discussed in this Article involves defining the duplication rights so

tent server, involved in a Web transaction: an ultimate consumer, C; another Internet server that provides pointers on its Web pages to the content server, PS; and fire wall computers, F.

First, suppose C initially establishes a session with PS to locate material of interest. C finds on PS a pointer to an item on CS. C clicks on this pointer. As a result, PS automatically uploads the selected pointer (in the form of a URL) to C's computer.¹⁵⁶ Now, the Web-browser software running on C's computer automatically establishes a connection with CS and retrieves the Web file pointed to by the pointer. C's Web browser caches the retrieved file so that if C requests it again, the cache copy can be loaded in the browser, rather than the browser having to fetch the file again over the Internet. In this transaction, PS never had the requested file, either before or after C requested it. Any downloading and caching occurred on the Web-browser application running on C's client computer.

As a second example, suppose that C's computer connects to a Local Area Network that in turn connects to the Internet through a fire-wall computer. While there are a variety of fire-wall configurations, a common one would cause the fire-wall to serve as a "proxy" for C. The popular Web-browser software has a proxy option to accommodate such a fire wall role. The proxy function is best defined by describing how it works in a Web transaction. C seeks to establish a connection to PS. The connection request is forwarded to F, which duplicates the request. Any information returned by PS, including the pointer, is transferred to F. F then caches the information and sends a copy along to C. When C's computer activates the pointer to CS, CS returns the requested file to F, which caches it, and sends a copy along to C. C also caches it because it is running the same Web browser as in the first example.

Some Web browsers, such as Netscape, keep the cached material even after the user exits the browser. The next time the browser runs, the cached files are available to it. An expiration date, included in the files sent by CS, determines how long a browser uses a cached version rather than reloading from the server from which the material originated. CS sets this expira-

that it does not cover caching; an alternative approach would be to define a new privilege, or to amend the fair-use privilege so that it covers caching.

¹⁵⁶ Actually, the page containing the pointer already had been uploaded into C's computer.

tion date, but the recipient may change it.¹⁵⁷ Thus, it is not factually correct to conceive of the browsers'—and the fire walls'—caching as ephemeral or transitory.

As a third example, consider an information-services provider such as CompuServe, Prodigy, or America Online. Such a service provider might want to provide Web access to its customers so that information retrieved through the Web would be more or less indistinguishable from material retrieved from the provider's host computer. The provider would almost certainly also cache the Web material on the provider's *host*, so that if another subscriber wishes to retrieve the same material, the second subscriber could do so directly from the provider's host computer, without the host having to go out and fetch the material again across the Internet.

Despite the engineering benefits of these three types of caching—faster response and less traffic on the network—all three types involve reproduction and thus potential copyright liability. The uncertainties confronting intermediaries can lead to a kind of de facto prior restraint on controversial content. The possibility of such prior restraint should stimulate more careful consideration of the tension between First Amendment and intellectual-property interests.¹⁵⁸

Even a fault-based standard forces an intermediary to be the judge of a copyright-infringement allegation. A mere allegation or rumor of infringing content may constitute "knowledge," thus exposing the intermediary to increasing damages the longer it permits the content to be disseminated through its service. Investigation and adjudication of copyright cases are expensive and require legal expertise. Because intermediaries face almost no liability if they remove a particular item or a pointer to that item, the economics of intermediary services dictate that in almost all cases, the intermediary simply will stop disseminating an item merely on accusation or rumor of infringement.

Even in those instances in which a particular configuration of technology reduces the risk of no-fault direct infringement, as in the Web without server caching, intermediaries potentially are exposed to liability as contributory infringers. For example, a request to suppress certain material might give the intermediaries sufficient knowledge to make them liable for contributory infringement under the *White Paper* formulation.

¹⁵⁷ See <http://www.ics.uci.edu/pub/ietf/http/draft-ietf-http-v10-spec-00.txt>.

¹⁵⁸ See Part VI for further analysis of First Amendment issues.

The *White Paper* acknowledges that the nature of increasingly complex intermediation technologies makes it infeasible for many intermediaries to check out the bona fides of the information they assist in disseminating. It may be feasible for a service provider that actually maintains copies of files and messages on its own computer to screen for offensive words or identifiable files. It certainly is not feasible, however, to automate screening for copyright or trademark infringement, especially for a provider who merely points to information resources created and maintained by others or who merely uploads textual files. Any attempt at such screening would clog up the dissemination technologies and dissipate their power. "Fair-use" arguments are subtle and cannot be decided by a computer algorithm, much less an automated filter that cannot possibly "know" enough about the surrounding circumstances to determine whether a particular file or message infringes someone else's copyright. Because of the volume of messages, inquiry into detailed factual circumstances would impose a major burden on providers.

Thus, de facto prior restraint will occur because of the combination of the rules of intermediary liability for copyright infringement and the economics of intermediaries in the information infrastructure. The intermediary will likely impose prior restraint at the first hint of a controversy over intellectual property. The intermediary is subject to an injunction or criminal prosecution in advance of the dissemination, and the possibility of a damages judgment works to shut down the dissemination just as effectively.

If courts give intermediaries more guidance as to what does and does not expose them to liability, and if the law insulates an intermediary from damages unless and until the intermediary receives a neutral determination that a particular item is infringing, the de facto prior-restraint threat would be reduced.

IV. ENCRYPTION'S POTENTIAL

Encryption is attractive as a way of reducing free-riding potential without heavy reliance on intellectual-property law and without relying unduly on intermediary liability. However, there are important limitations on encryption as a solution.

Content encryption extends technical protection beyond value-added processes to the content itself. A variety of proposals for digital libraries would rely on encrypted content in order to make

the otherwise public good excludable.¹⁵⁹ They all rely on the basic concept that one can decrypt the desired information content only by using a key for which one would have to pay. Encryption applications deploy systems that would limit the number of times encrypted content could be accessed. The systems also would permit certain types of use and exclude other types, such as replication. Such encryption applications increase the pirate's c_a , potentially to infinity. The same applications permit one to determine with high reliability whether content has been altered, such as by the removal of various notices and advertisements.¹⁶⁰ The applications increase the pirate's c_{II} .

Encryption has important limitations, however, that prevent its use as the main means of protecting intellectual property in the information infrastructure. Encryption works only when both the producer and the consumer of information adhere to the encryption standards. Nothing in the history of developing standards for computer formats suggests optimism about the feasibility of developing a truly universal standard for encryption.¹⁶¹ Nor is it feasible or desirable for the government to mandate adherence to such a standard. Such a mandate would put the government in the position of prohibiting expression except through the approved encryption standard, and that would raise insuperable First Amendment problems. The experience with the proposed Clipper-chip initiative discourages enthusiasm about the potential for government-led standardization of encryption methods. The original proposal did not contemplate mandating the use of the Clipper standard. Nevertheless, the outcry against it was so great that it had to be withdrawn.¹⁶²

Moreover, any method of encryption has adverse implications for information-system performance or reliability. Copy protection

¹⁵⁹ Karen Frank and Michael Higgins, *Fair Use: In the Courts and Out of Control*, 411 PLI/PAT 1 (1995).

¹⁶⁰ See Marvin A. Sirbu, *Internet Billing Service Design and Prototype Implementation*, Proceedings: Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment 67 (Interactive Multimedia Association, Jan 1994).

¹⁶¹ See Henry H. Perritt, Jr., *Format and Content Standards for the Electronic Exchange of Legal Information*, 33 Jurimet J 265 (1993) (explaining the dynamics of private standard setting).

¹⁶² In July 1994, the Clinton Administration abandoned its original clipper proposal. The Vice President announced that the original Clipper-chip technology would be used for telephone communications, but that the Administration would launch a five-month study to develop a new encryption initiative for computer use. The new proposal would be voluntary, would not rely on a classified algorithm, and would be exportable. Holly Bass, *U.S. Scales Back Encryption Plan for Computers*, Wall Street J B5 (July 22, 1994) (reporting on letter from Vice President to Representative Maria Cantwell).

of desktop-computer software revealed how strongly consumers resist these limitations. In the face of such consumer resistance, copy protection that was commonplace in 1985 had virtually disappeared from mass-marketed computer software by 1995. One can expect the same kind of resistance with respect to encryption arrangements that sometimes block access by authorized users and impede performance.

For those markets in which consumer resistance impedes more profitable and larger scale electronic publishing, adding a technological basis for additional consumer resistance likely will not appeal to entrepreneurs who want market development. In other words, encryption may increase the originator's c_m more than it increases the pirate's c_a .

Undue reliance on encryption solutions to intellectual challenges could produce a plethora of incompatible encryption systems. A collection of technically isolated archipelagos would exist, rather than a national information infrastructure, much as the online information services like CompuServe, America Online, Lexis/Nexis, Dialog, and Westlaw existed in isolation from each other before the NII encouraged interconnections and gateways.

Encryption technology is best used not to protect content, but to facilitate payment systems so that unencrypted content may be sold cheaply in open network architectures.

V. SOLUTIONS

A regime that protects intellectual property and also shelters new creative and productive exploitation of information must target realistic transaction costs that impede bargaining. The attributes of public goods justify the artificial property constructs of copyright and patent law. The best policy is to leave copyright law intact, develop a richer array of pricing and business models for electronic publishing, develop private cooperative arrangements for licensing and policing intellectual property, and extend the infrastructure for electronic-payment systems.

If the Copyright Act is amended, it should be amended not only to extend protection for content originators, as the *White Paper* suggests, but also to offer certain immunities for intermediaries in open network architectures, and to strengthen the role of the First Amendment.

A. Proposals for Expanded Legal Protection Are Unsupported

The Administration's *White Paper* mistakenly addresses new technological threats to intellectual property through the law and through expanding protection for content originators, and it minimizes the concerns of consumers and intermediaries. While claiming an intent only to "clarify," the *White Paper* recommends the establishment of a new transmission right in copyright law:

It is not clear under the current law that a transmission can constitute a distribution of copies or phonorecords of a work. Yet, in the world of high speed communications systems, it is possible to transmit a copy of a work from one location to another. This may be the case, for instance, when a computer program is transmitted from one computer to ten other computers. When the transmission is complete, the original copy typically remains in the transmitting computer and a copy resides in the memory of, or in storage devices associated with, each of the other computers. The transmission results essentially in the distribution of ten copies of the work. However, the extent of the distribution right under the present law may be somewhat uncertain and subject to challenge. Therefore, the Working Group recommends that the Copyright Act be amended to expressly recognize that copies or phonorecords of works can be distributed to the public by transmission, and that such transmissions fall within the exclusive distribution right of the copyright owner.¹⁶³

According to the *White Paper*, the proposed amendment simply "recognizes" the appropriate scope of the distribution right.¹⁶⁴ In the view of the Working Group, the amendment is necessary, among other things, to make it clear that distribution in the form of transmission is the exclusive prerogative of the copyright owner. The distribution right as currently interpreted covers only "publication."¹⁶⁵

¹⁶³ United States Department of Commerce, Information Infrastructure Task Force, *Intellectual Property and the National Information Infrastructure: Report of the Working Group on the Intellectual Property Rights 192-93* (Sept 1995) ("*White Paper*") (cited in note 5).

¹⁶⁴ *Id.* at 193.

¹⁶⁵ *Id.* at 195.

The *White Paper* rejects any special safe harbors for intermediaries. While recognizing that intermediaries, such as online service providers and Internet servers, "play an integral role in the development of the NII and facilitate and promote the free exchange of ideas,"¹⁶⁶ the *White Paper* suggests that this should not be grounds for removing or reducing liability for copyright infringement. "One can perform these functions without infringing or facilitating the infringement of the copyrighted expression of others."¹⁶⁷ The *White Paper* further argues that intermediaries remain in the best position to detect copyright infringement, and that they could shift any undue risk of strict liability to their customers or suppliers through routine contracting arrangements.¹⁶⁸

The *White Paper* is troubling because it suggests that fair use has a narrow scope. It misleadingly de-emphasizes the role of exploitation of information by downstream authors and publishers as a core part of copyright analysis. In a similar vein, the *White Paper* overemphasizes the scope of vicarious liability under doctrines such as contributory infringement. The *White Paper* jumps to the conclusion that more legal protection is needed without carefully probing the technological and marketing underpinning of such a conclusion.

A number of intellectual-property scholars proposed, in an extensive article published by the Columbia Law Review in late 1994,¹⁶⁹ a new system of protection for computer works. While this *Manifesto* is an incisive starting point for reconsidering the opposing positions in the controversy over protection of "look and feel" in computer program functioning,¹⁷⁰ it is of only limited use in shaping an appropriate form of property for information content. The *Manifesto* characterizes computer programs as processes. The distinction between computer programs and computer

¹⁶⁶ Id at 105.

¹⁶⁷ *White Paper* at 105 (cited in note 5).

¹⁶⁸ Id at 105-06.

¹⁶⁹ Pamela Samuelson, et al, *A Manifesto Concerning the Legal Protection of Computer Programs*, 94 Colum L Rev 2308 (1994) (the "*Manifesto*").

¹⁷⁰ The *Manifesto* authors started from the proposition that computer programs "behave." Id at 2316. The *Manifesto* authors proposed a blockage period for clones, although they were somewhat ambiguous as to its length. Id at 2414. The blocking period could differ for different types of original work in clones. It would allow third-party development but not distribution during the blocking period. A system of registration could extend the blocking period. Id at 2418. This would be a "light" registration system, more like copyright than patent, in that there would be no examination. Samuelson, 94 Colum L Rev at 2417 (cited in note 170).

data is likely to become even more indistinct than at present, as html tags embody more procedural information and as object-oriented systems such as Java become more common. Information content, however, will remain more like data than programs. As such, a process-oriented intellectual-property regime is largely immaterial to protection of content contributors. Nevertheless, the *Manifesto* represents a more useful contribution to the policy dialogue than the *White Paper*. The *Manifesto* seeks to work out legal protections to fill actual gaps in technological protections of creative effort, rather than jumping to the conclusion that an expanded role for the law is desirable.

B. Embrace New Pricing and Business Models

Protecting intellectual property in a flourishing NII depends more on the imagination of entrepreneurs in designing and deploying new business and pricing models than on legal creativity. Radio and television patterns should be imitated; they were the last big revolution in information technology and necessitated changes in the way intellectual property was handled. To be sure, radio and television entrepreneurs did not forswear intellectual property, but traditional notions of copyright fit poorly because radio and television programming was not distributed in the form of tangible copies. To respond to these challenges, the entrepreneurs radically changed the location of the tollgate.¹⁷¹

In cyberspace, new tollgates and new ways of pricing will enable content contributors to earn a fair return while undercutting efforts by pirates to free ride. For example, the costs of extracting large amounts of content from finely grained retrieval systems can be substantial. If persons cooperate in the marketing of information through such systems and set a price that is not much greater than a pirate's costs to extract the information unlawfully,¹⁷² then the economic incentives for piracy diminish. Alternatively, block pricing for access to licensed content on a nonexclusive basis reduces transaction costs¹⁷³ for content contributors and intermediaries. As their transaction costs diminish,¹⁷⁴ the margin for a pirate diminishes as well.

¹⁷¹ See Note, *Coming to Terms with the Celestial Jukebox: Keeping the Sound Recording Copyright Viable in the Digital Age*, 74 BU L Rev 505, 513 n 45 (1994) (noting that broadcasters have historically opposed performance rights).

¹⁷² That is, if $P = c_a + c_m + c_r$.

¹⁷³ These transaction costs are c_m .

¹⁷⁴ This decreases the originator's c_m and c_r .

The spread of nonexclusive publishing arrangements can assure content contributors a greater return because of larger markets. At the same time, these arrangements reduce the likelihood of closed systems swamping a surrounding open network architecture and reduce piracy incentives because content is available to a wider variety of intermediaries who competitively serve demand better.¹⁷⁵ Already, the popularity of the Internet has changed bargaining power and bargaining positions between content providers and intermediaries.¹⁷⁶ Whether or not authors agree to exclusive contracts with their publishers is purely a matter of bargaining power and practice.¹⁷⁷

C. Methods of Protecting Content and their Classification

World Wide Web technologies permit the originator of content to protect her investment without relying entirely on intellectual property. These new technology-enabled methods, summarized in Figure 4, fall into three overlapping categories: product design, business models, and technology.

All three methods reduce the nonexcludability and nonrival characteristics of content sold by itself.¹⁷⁸ Product-design methods include planned obsolescence, finer granularity, addition of presentation markup, bundling vulnerable material to less vulnerable value-added elements, and concentrating investment on value-added features other than content. Planned obsolescence decreases the value of the content item that might be subject to piracy. By the time the pirate brings his copy to the market, consumers will prefer a more current version from the originator.

¹⁷⁵ See Steve Lohr, *On-Line Stars Hear Siren Call of Free Agency*, NY Times 37 (Nov 25, 1995) (cited in note 116) (reporting on growing tendency of content originators, including discussion-group organizers, to move away from exclusive arrangements with CompuServe and America Online into nonexclusive distribution through the Internet).

¹⁷⁶ See Business Wire, *Times Will Move TimesLink to the World Wide Web* (Sept 27, 1995) (describing Los Angeles Times bypassing Prodigy and publishing directly on the Internet's World Wide Web).

¹⁷⁷ For example, this author regularly accedes to exclusive arrangements with his book publishers, simply because that is the way business is done in book publishing, and book publishers would be very reluctant to accept a nonexclusive contract. On the other hand, the author usually extends only a nonexclusive license to law reviews that publish his articles, because law-review licensing practice is less firmly established, and the author has greater leverage.

¹⁷⁸ Some transaction costs, like nonrivalness and nonexcludability, make it more difficult for originators to strike and enforce a bargain that will allow them to recover their investment. Other transaction costs help the originator distinguish between his grantee and a pirate, reduce the nonexcludability characteristic of his product, and therefore enhance his ability to protect his investment.

Finer granularity and the addition of presentation markup increase c_i because the pirate must assemble more grains and remove presentation markup. Finer granularity also may increase c_a because more human intervention likely will be needed to download a marketable amount of material.¹⁷⁹

Bundling vulnerable material to less vulnerable value-added elements increases c_a because it becomes more difficult for the pirate to get to the content he wishes to steal.¹⁸⁰ Shifting investment toward value-added elements and away from content might seem inefficient because it would result in the underproduction of content. But different ways to satisfy consumer needs exist, some exposing the originator to a lower risk of free riding. For example, one can author a work so that different structural components are identified by transitional language in the text. Alternatively, one can segment the work and make different parts retrievable separately. Writing the work so that its segments can be identified by text means that investment in structural differentiation is made in the form of compensation to the author. If one segments the work, one can invest separately in content authorship and the tags, pointers, and software that retrieve the individual segments and link them together. The value-added features are inherently more excludable, potentially confronting the pirate with very high c_a and c_i .

A number of feasible business models exist in the Web and compensate for remaining nonrival and nonexcludability characteristics of content. The producers of downstream value may make subsidy payments to content producers in order to draw customers to their access and retrieval systems. They can reduce the necessary outlays if they cooperate with other producers of downstream value and make nonexclusive arrangements with content producers. A variety of institutional arrangements are also conceivable. Content producers could give global licenses in exchange for a share of aggregate revenues flowing to all producers of downstream value. Third parties could subsidize the production of content, as in the business model for television, radio

¹⁷⁹ The development of robots that permit one to point to an item on the Web and to automatically retrieve all related Web items potentially frustrates finer granularity as a way of increasing a pirate's c_i . But, techniques also exist for excluding some or all robots from Web sites. See Martijn Koster, *Robots in the Web: threat or treat?*, <http://info.webcrawler.com/mak/projects/robots/threat-or-treat.html>.

¹⁸⁰ See Australian Office of Regulation Review, *Economic Analysis Of Copyright Reform 45* (1995) (describing intellectual property "tie-ins" as means of protection) (cited in note 25).

broadcasting, and newspapers. Proprietors of electronic markets, such as automated help-wanted advertising sections, can buy content in order to attract customers to their markets.

Technology also permits direct changes in the degree of excludability and nonrivalness. In Westlaw and CompuServe, information is excludable because the electronic gateway into the computers through which information is dispensed does not allow consumers and potential pirates into the system unless they have an account. Consumers must pay the bill to maintain their account. The same concept can be deployed in the Web. Particular items of information may be protected by passwords on certain Web pages by automating the login process for those particular pages.

Commentators have proposed a variety of methods for content encryption and copyright management that use technology not only to make information excludable, but also to make it rival. One person's use thus defeats the use entitlement of the predecessor.¹⁸¹

Technology also can reduce transaction costs for exchanges between buyers and sellers of information. For example, VISA and Mastercard recently published standard documents for credit card transactions on the Internet. These documents likely will hasten the deployment and use of payment systems that permit low-cost exchanges of chunks of information so small that they are not worthwhile to steal. Thus, the payment-system technology and product design together reduce the relative transaction costs to payers and increase the acquisition and transformation costs for nonpayers.

D. The Role of Private Cooperatives

Historically, copyright-licensing collectives have played a useful role in reducing the transaction costs of disseminating intellectual property to authorized redistributors¹⁸² and in reducing the costs of detecting violations.¹⁸³ The American Society of Composers, Authors, and Publishers ("ASCAP"),¹⁸⁴ Broadcast

¹⁸¹ See generally *Proceedings: Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment* (Interactive Multimedia Association Intellectual Property Project, 1994) (collecting nineteen papers that describe technological means for controlling and metering access to information in electronic formats).

¹⁸² This decreases c_m .

¹⁸³ This increases c_{ij} .

¹⁸⁴ *United States v American Society of Composers, Authors and Publishers*, 32 F3d 727, 728 (2d Cir 1994) (describing ASCAP's role in collecting fees for broadcast jingles);

Music, Inc. ("BMI"),¹⁸⁵ and the newer Copyright Clearance Center ("CCC")¹⁸⁶ have demonstrated their capability in this regard. Similar institutions can arise in the electronic environment, although they have not done so yet.¹⁸⁷ It is useful to identify the possible functions and configurations for copyright collectives in environments like the Web.

1. *Detect violations.*

An intellectual-property cooperative can assist enforcement by detecting infringement. The cooperative could monitor advertisements and other promotional efforts by pirates, sample the virtual places in which infringement is likely,¹⁸⁸ and visit places in which jukeboxes and newer technological means are installed.¹⁸⁹

The cooperative could deploy "sniffers" that would detect bit patterns suggestive of infringing conduct. For example, if legitimate publishers use a common signature or trademark to signify authorization to publish copyrighted works, the sniffer could look for instances of that bit pattern transmitted by unauthorized servers on a network. Or, in the case of extremely popular works, the sniffer could look for bit patterns representing unique or nearly unique parts of the content, transmitted by unauthorized sources.

Superhype Publishing, Inc. v Vasiliou, 838 F Supp 1220 (SD Ohio 1993) (imposing vicarious liability on restaurant for playing music without license from ASCAP).

¹⁸⁵ *Broadcast Music, Inc. v Claire's Boutiques, Inc.*, 949 F2d 1482, 1484 (7th Cir 1991) (describing BMI and holding that defendant was not liable for copyright infringement for playing music in stores); *International Korwin Corp. v Kowalczyk*, 855 F2d 375, 381 n 12 (7th Cir 1988) (describing BMI and comparing it to ASCAP); *Broadcast Music, Inc. v Opticom Inc.*, 1992 WL 510894 (ED Va) (describing how BMI investigator recorded unlicensed broadcasts).

¹⁸⁶ *American Geophysical Union v Texaco, Inc.*, 60 F3d 913, 929 n 16 (2d Cir 1994) (describing CCC); *Copyright Clearance Center, Inc. v Commissioner of Internal Revenue*, 79 Tax Ct 793, 795 (1982) (describing functions of CCC).

¹⁸⁷ See Robert P. Merges, *Of Property Rules, Coase, and Intellectual Property*, 94 Colum L Rev 2655, 2662 (1994) (arguing that presence of high transaction costs can encourage producers and users to invest in institutions that lower the cost of certain types of exchanges; citing radio broadcasting as historical example) (cited in note 59). See also Robert P. Merges, *Intellectual Property and the Costs of Commercial Exchange: A Review Essay*, 93 Mich L Rev 1570 (1995) (arguing for development of integrated commercial-law doctrine for intellectual property-based transactions).

¹⁸⁸ This is analogous to BMI's monitoring of radio broadcasts.

¹⁸⁹ See *Broadcast Music, Inc. v Star Amusements, Inc.*, 44 F3d 485, 486 (7th Cir 1995) (describing role of BMI and ASCAP in enforcing copyright with respect to jukebox operators).

Despite the possibility of such technological detection of infringement, more attention should be given to practical implementation. For example, a sniffer computer must have the capacity to process all of the packets traversing its network segment. This means that a sniffer positioned astride a major stream of Internet commerce, as on a backbone or network access point ("NAP"),¹⁹⁰ must have processing capacity equal to the routers making up the backbone or NAP service. While a lower-capacity sniffer could handle all of the packets moving through a particular midlevel network, it would never see potentially infringing packets moving on other midlevel networks. The cost of a comprehensive infringement-detection system would depend not only upon the cost of developing and deploying an appropriate pattern-matching algorithm, but also upon the number of backbone connections or NAPs and the cost of replicating backbone or NAP processing speed.

2. *Standardize licensing terms.*

Intellectual property cooperatives can standardize terms for licensing for common activities such as caching. For example, a cooperative could extend an offer to all Web intermediaries that, in exchange for the payment of a fixed and modest amount, it would authorize the intermediaries to engage in a defined type of caching as to all the intellectual property represented by the cooperative. Then, the placement of a work on a Web server by a content originator represented through the cooperative implies (or expressly gives) authorization to engage in the defined caching. In addition, it provides a low-cost and low-risk way for intermediaries to reduce the risk of infringement liability.

3. *Simplify pricing.*

Cooperatives can simplify pricing for the use of represented works. Much as film libraries make it easier for republishers and creators of derivative works to access existing film footage, an electronic intellectual-property cooperative could organize pointers to represented works and offer standard pricing arrangements for persons wishing to disseminate or adapt those works.

¹⁹⁰ As the Internet has become commercialized, the concept has shifted from a hierarchical network model, in which midlevel networks are connected to each other through one or more backbones, to a model in which midlevel networks connect directly to other midlevel networks through NAPs. See National Science Foundation RFP.

4. *Provide certificate-authority services.*

One of the prerequisites to an effective public-key encryption system is the availability of public keys for all participants. Under RFC¹⁹¹ 1122, "certificate authorities" ("CAs") associate participant names with their public keys in a way that reduces or eliminates the potential for spoofing and impersonation.¹⁹² A copyright cooperative could function as a CA for content owners who encrypt either their content or their header information that identifies licensing terms.

Intellectual-property cooperatives could expand beyond the provision of public-key encryption CA services into a broader range of electronic payment system services. Most proposals for electronic payment systems rely on some form of public-key encryption, and it is logical for the CA to provide payment authorization services similar to those performed by credit card authorization services.¹⁹³

E. Law's Role

The best solution for legal protection is to leave present law alone. The *White Paper* does not make the case for establishing a new transmission right, and no justification exists for American adoption of database protection measures like those recommended by the European Commission. There is every reason to believe that the product design, business method, and technological protections addressed in Part IV.C will increase c_a and c_i so as to leave present levels of c_{ll} adequate to protect originator investment. Congress should reject the recommendations of the *White Paper* and leave the present copyright statute intact.

A healthy information infrastructure undoubtedly requires adequate legal protection for the intellectual property of content creators. While extending the scope of copyright protection, as recommended in the *White Paper*, might maximize the position of existing intellectual-property owners, such extension would not necessarily optimize the production and use of information. The extension of protection for existing intellectual property represents a barrier and a cost to creators of new intellectual property.

¹⁹¹ An RFC is a statement of a technical standard for the Internet. RFCs are developed by the IETF.

¹⁹² S. Kent, *Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management: RFC 1422* (Network Working Group, 1993).

¹⁹³ See Henry H. Perritt, Jr., *Legal and Technological Infrastructures for Electronic Payment Systems*, 22:1 Rutgers Computer and Technology L J 1 (1996).

At any point on a continuum of intellectual-property protection, some creators will always find adequate incentive and acceptable risk of piracy and therefore will create and produce, while others will find the risks too great or the rewards too small. Thus, at almost any conceivable scope of copyright and other statutory protection, some level of electronic publishing and Internet-like environments will exist. Some potential authors and publishers, however, will always claim that they will only add to the store of electronic information if the law is changed. Congress should not change sound policy and sound law merely because some potential contributors testify that the status quo frightens them. Rather, Congress should scrutinize the empirical evidence of actual and withheld resources and seek to discover links between conduct and the state of the law. A single maximum for social welfare does not, and will never, exist. Rather, an evolving boundary between the protected and the unprotectable will exist, shaped by a political equilibrium among competing economic interests.

It is reasonably clear, however, that something more or less like today's copyright, trade secret, trademark, and contract protections should continue to operate. These legal entitlements protect content originators from gross piracy.

New business and pricing models, supplemented by electronic payment systems, are likely to be adequate to stimulate development of rich content in the Global Information Infrastructure (GII). These methods are far less likely to stunt development of the crucial intermediary function in the GII than the *White Paper's* recommendations.

If the law *is* changed, statutory protection for intermediaries, especially for caching, should be added. The possibility of primary or contributory copyright-infringement claims against Internet intermediaries may result in a kind of de facto prior restraint that interferes with a lively information marketplace in open network architectures. Statutory protection for intermediaries may be an appropriate piece of a comprehensive statutory approach to intellectual property in the NII, notwithstanding the difficulty of defining the types of caching that deserve protection. Both a safe harbor for caching and stronger protections against ex parte seizure orders may be appropriate.

Just as the case has not been made for amending the Copyright Act to extend protection for copyright owners, neither does the case law cry out for new statutory protections for intermediaries. Only two cases actually imposed no-fault liability on intermediaries, and their factual situations suggested that the inter-

mediaries deserved liability, even though fault may not have been provable. The different legal position of traditional online service providers who maintain their own content and do their own copying and distribution in response to consumer requests, compared with Web servers, may create a healthy migration away from older technologies to newer ones like the Web. This migration would unbundle the intermediary function from the content-originator function, and thus perhaps make it easier to target indemnification and other practical arrangements that protect pure intermediaries. As the *White Paper* states, content servers may be indemnified by their customers who place content on them.

On the other hand, if Congress amends the Copyright Act to adopt the suggestions expressed in the *White Paper*, it certainly also should amend the Copyright Act to recognize the intermediaries' needs for safe harbors. Communications law, written into the Copyright Act, offers a useful model for such statutory protection. The Copyright Act deals with the special position of intermediaries in its provisions concerning specialized privileges for broadcast intermediaries. For example, section 111(a)(3) provides that copyright infringement does not occur if a secondary transmission embodying a performance or display of a work is made by:

any carrier who has no direct or indirect control over the content or selection of the primary transmission or over the particular recipients of the secondary transmission, and whose activities with respect to the secondary transmission consist solely of providing wires, cables, or other communications channels for the use of others.¹⁹⁴

The legislative history notes that Congress intended section 111(a)(2) to grant a privilege to "passive carriers."¹⁹⁵ Section 111(a)(1) provides a similar privilege for secondary transmissions to parts of a hotel, apartment house, or similar establishment, but only so long as no alterations are made.¹⁹⁶

Intermediaries in the NII play a somewhat different role from transmission facilities in broadcast media. Intermediary protection must recognize a system operator's selection of class-

¹⁹⁴ 17 USC § 111(a)(3) (1994).

¹⁹⁵ See HR Rep No 94-1476, following 17 USC § 111 (1994).

¹⁹⁶ 17 USC § 111(a)(1) (1994).

es of communications to conform to its entrepreneurial definition of its product or service niche. It also must recognize the appropriateness of certain transformations and alterations that occur as part of normal digital processing. One could adapt the language of section 111 to the position of other kinds of intermediaries in the NII in the following way:

[F]orwarding or transferring a work infringing the copyright of another does not itself constitute copyright infringement if the forwarding or transferring is made or facilitated by an electronic service provider who has no direct or indirect control over the content of the infringing work and whose activities with respect to the forwarding consist solely of providing communications channels, pointers, and intermediate copying at the request of another or for the use of others. This exemption shall not extend to sponsoring, soliciting, promoting, or adopting infringement as the provider's own.

Even if Congress does not grant more general immunity for intermediaries, caching represents a particularly compelling case for a safe harbor. In all three examples given in Part III, it seems appropriate to classify the caching as consistent with the assumed restrictions on use of the content. In other words, the described caching should not be considered illegal copying. Courts can avoid infringement for caching by defining certain types of caching as fair use or by concluding that an implied license to cache exists.

However, such privileged caching is difficult to define. Limiting the privilege to ephemeral copies would be too narrow because of the way Netscape caches to disk and preserves cached files after a Netscape session is terminated. Extending the privilege to copies made to facilitate future retrieval might be too broad because such a privilege could frustrate a content supplier's legitimate interest in restricting secondary copying. For example, the provider in the third example offered in Part III might allow its customers to obtain material from its host without paying for access to the material from CS. Or, C might pay once for an access to CS, but then obtain another copy from the cached version on the provider's host and make prohibited copies of that second cached copy. C could argue that the restrictions applicable to the original accessed material do not apply to material accessed from the provider's host. It might be appropriate to condition the privilege on not using the cached version to inten-

tionally or foreseeably frustrate the restrictions imposed by the content supplier with respect to third parties. While Congress could specify the details of a caching privilege in a statute, it would be better to work them out through a private cooperative licensing scheme as suggested in Part V.B.

Coasian analysis suggests that it may not matter whether intermediaries face liability if they can bargain to shift the liability elsewhere. The *White Paper* assumes that intermediaries can shift the liability. Calabresi and Melamed offer five considerations for placing entitlements:

(1) that economic efficiency standing alone would dictate that set of entitlements which favors knowledgeable choices between social benefits and the social costs of obtaining them, and between social costs and the social costs of avoiding them; (2) that this implies, in the absence of certainty as to whether a benefit is worth its costs to society, that the cost should be put on the party or activity best located to make such a cost-benefit analysis; (3) that in particular contexts like accidents or pollution this suggests putting costs on the party or activity which can most cheaply avoid them; (4) that in the absence of certainty as to who that party or activity is, the costs should be put on the party or activity which can with the lowest transaction cost . . . correct an error in entitlements by inducing the party who can avoid social costs most cheaply to do so; and (5) that since we are in an area where by hypothesis markets do not work perfectly—there are transaction costs—a decision will often have to be made on whether market transactions or collective fiat is most likely to bring us closer to the pareto optimal result.¹⁹⁷

The fourth criterion is particularly significant. Who has the lowest transaction cost in negotiating a shift in liability?¹⁹⁸ The originator's intermediary faces relatively low transaction costs for negotiations with the originator because the intermediary either acquires the originator's content and places it on his own server, or establishes pointers to the originator's server. These transaction costs may be high or low relative to the value of the

¹⁹⁷ Guido Calabresi and A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 Harv L Rev 1089, 1097-98 (cited in note 7).

¹⁹⁸ Figure 3 introduces the entities discussed in the following paragraphs.

content, but they are surely lower than anyone else's vis-a-vis the originator. The consumer faces the lowest transaction costs for negotiations with the consumer's intermediary. The consumer has an account with the consumer's intermediary, or at least the consumer's intermediary has an opportunity to exclude the consumer—based on the consumer's IP address.¹⁹⁹

The pure intermediary faces the highest transaction costs for negotiations with either originator or consumer. The intermediary does not know who the originator or consumer is, and cannot know in advance of a request from a particular consumer for a particular piece of content traversing the pure intermediary's server. The originator and consumer also face relatively high transaction costs with respect to negotiations with each other because neither knows who the other is in advance and neither may have the opportunity to know because the transaction occurs through a series of intermediaries. Thus, it should not make any difference whether one grants an entitlement to an originator or an originator's intermediary because they can negotiate a reallocation of responsibility between them. Similarly, it should not matter whether one imposes a duty on the consumer or the consumer's intermediary because they likewise can negotiate a reallocation. The problems exist with respect to reallocation between the originator end and the consumer end. The validity of the *White Paper's* conclusion depends upon the pure intermediary having lower transaction costs for negotiating than either the originator and its intermediary or the consumer and its intermediary. A pure intermediary could have lower transaction costs only if its size were such that it would have greater knowledge than originators, consumers, or both.²⁰⁰

This leaves the question of whether property or liability rules are most appropriate. Professor Hardy's article suggests that new information technologies reduce transaction costs, and therefore a shift to property rules may be appropriate.²⁰¹ This suggests less reliance on trade secret and more reliance on copyright, patent, and trademark. It also suggests less reliance on contract, as with Westlaw or America Online.²⁰² One could

¹⁹⁹ But this is not unique because, given the way the Web works, any server knows who the consumer is and has the same opportunity to exclude a request from that IP address. So the consumer's intermediary may not be special after all.

²⁰⁰ Lack of knowledge is a transaction cost in the Coasian framework.

²⁰¹ Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U Chi Legal F 217, 219 (cited in note 8).

²⁰² Licensing is a liability-based approach because it relies on contract law, and the

argue that what matters is not the *absolute* level of transaction costs, which probably decreases with new information technology, but the *relative* level of transaction costs, given the value of items of information to be exchanged. Thus if new uses of information technology decrease the value of the items to be exchanged, as they may when granularity becomes finer, then a shift in favor of property rules would be appropriate only if transaction costs decrease faster.

Notwithstanding the aforementioned difficulties, encryption plays a role in protecting intellectual property. Some content originators will prefer technological protection through content encryption and/or encryption systems associated with payment systems and license and registration authentication schemes, considered more fully in Part V.C., licensing cooperatives can use encryption to authenticate intellectual-property permissions and to limit certain intellectual-property publishing to members of the cooperative. Such encryption systems also can facilitate detection of violations and thus make legal protections more enforceable. More important, encryption can be used for authentication in electronic payment systems.

Acceptable payment systems require encryption to assure the privacy of information such as credit card numbers and to protect sellers against forgery. Public-key encryption (also known as asymmetric-key encryption) seems to be the most appropriate tool with which to build payment systems. Private-key encryption produces as good or better security and authentication with better performance. However, private-key encryption is poorly suited to open systems like the Internet, where sellers and buyers want to do business with each other without having any prior relationship. If private keys had to be exchanged before single-key encryption transactions, a prior relationship would be necessary.

traditional remedies for breach of contract are damages rather than injunctions. Property rules are enforceable by injunction and thus require negotiation in advance of transfer. Liability rules allow a government institution such as a court to determine the value after the interest has been transferred. Calabresi and Melamed offer a picturesque illustration: "If we were to give victims a property entitlement not to be accidentally injured we would have to require all who engage in activities that may injure individuals to negotiate with them before an accident, and to buy the right to knock off an arm or a leg." Calabresi & Melamed, 85 Harv L Rev at 1108 (cited in note 7). See Merges, 93 Mich L Rev at 1574 (cited in note 188) ("The most obvious illustration of how property rights confer tight control is . . . the availability of quick injunctions in the event of breach."). Professor Merges argues that it is difficult for contract terms to substitute fully for the enhanced control conferred by the availability of injunctions for infringements of intellectual property. Id at 1574-75.

Encryption does not solve the problem, however, without the technological and legal infrastructure to support encryption in open network environments. Two encryption applications are of interest: making content unavailable to those without a key, and authentication and binding. Making content unavailable involves the same applications used to ensure message privacy. Authentication and binding involve digital-signature functions. Public-key encryption serves both privacy and digital signature functions. It uses two different keys for the same message, one of which can be made available to the public generally, and the other kept secret. To ensure privacy—or unavailability of content—the sender uses the recipient's public key to encrypt the message, which then becomes inaccessible to anyone lacking the corresponding private key—which only the recipient has. If a particular customer does not pay, the sender would not encrypt with that customer's public key. To verify that a message came from a particular source, and to detect any tampering with the parts of the file or message, the sender uses her secret key to sign a "digest" of the message. Anyone with that sender's public key can decrypt the message, but that public key will decrypt only digests coming from that sender. The same privacy and digital signature functions also make secure payment systems possible in open network architectures.

Widespread use of public-key encryption to protect intellectual property requires an infrastructure for key management. In order for public-key encryption to work in large open systems, there must be places from which public keys can be obtained and associated with the person or entity with whom one wants to do business. Most approaches to public-key encryption envision one or more public-key CAs that would maintain databases, somewhat like conventional telephone directories, that associate each potential sender with her public key. Though the CA could be corrupted, for example, by a crook masquerading as a credit card company to confirm a credit card order, it would become harder as more CAs develop. The more independent entities that must be corrupted, the greater the challenge for someone who wants to compromise security. Thus, by adding more independent verification institutions, one increases security even if no single entity is completely trustworthy.

Technological and legal questions associated with the key-certification process form the core of the infrastructure questions with respect to public-key encryption. The Internet community

has already addressed the technical issues,²⁰³ but the legal issues still must be resolved.

Utah recently enacted the first statute governing digital signatures.²⁰⁴ The Utah digital-signature statute establishes an authentication hierarchy that conforms to the authentication hierarchy of RFC 1422. The statute also establishes an administrative agency to regulate the authentication of computer-based documents.²⁰⁵

The Utah statute makes a digitally signed document as valid as if it had been written on paper,²⁰⁶ except for "a negotiable instrument payable to bearer" or financial-institution transactions.²⁰⁷ The statute establishes presumptions for certificates issued by licensed CAs and excludes certificates issued by unlicensed CAs. The statute presumes that a certificate is an acknowledgment of a digital signature, that a digital signature verified with a public key is affixed with the intention of the subscriber to authenticate the message and to be bound by its contents, and that a time-stamped digital signature is *prima facie* evidence that the signature took effect as of the date and time indicated. The presumption in favor of a digital signature's validity may be rebutted only under defined situations.²⁰⁸

²⁰³ Kent, *Privacy Enhancement for Internet Electronic Mail* (cited in note 193) (defining architecture and infrastructure for authentication system based on public-key encryption techniques).

²⁰⁴ Utah Digital Signatures Act, 1995 Utah Laws Ch 61. The Utah Digital Signature Legislative Facilitation Committee drafted the digital-signature statute to support several standards, including X.509 and RFC 1422. Utah Code Ann § 46-3-102(4) (1995) (referring to "Standard X.509 of the International Telecommunication Union (formerly CCITT or International Telegraph and Telephone Consultative Committee), . . . Standard X.9.30 of the American National Standards Institute (ANSI), and . . . RFC 1421 through 1424 of the Internet Activities Board (IAB)"). Utah's statute is optional in two respects: it makes registration of CAs optional; and it allows trading partners to use paper or to make any other form of payment arrangements they wish. Utah Code Ann § 46-3-201; *id.*, § 46-3-402.

²⁰⁵ This agency would be analogous to a Policy Certification Authority ("PCA") in RFC 1422. A PCA establishes and publishes policies for registering CAs and subscribers. For the Internet community, PCAs publish their policies in the form of informational RFCs.

²⁰⁶ Utah Code Ann § 46-3-402 (1995).

²⁰⁷ *Id.* § 46-3-403.

²⁰⁸ Section 46-3-401(5) provides that the presumption may be rebutted:

- (a) by evidence indicating that a digital signature cannot be verified by reference to a certificate issued by a licensed certification authority;
- (b) by evidence that the rightful holder of the private key by which the digital signature was affixed had lost exclusive control of the private key, without violating any duty imposed by this chapter, at the time when the digital signature was affixed;
- (c) by evidence showing a lack of a signature at common law; or
- (d) by a showing that reliance on the presumption was not commercially reason-

The Utah statute goes further than RFC 1422 in allocating the risk of a CA mistake. CAs that wish to be licensed in Utah must post a bond, and their liability in the event of a mistaken certification is limited to the amount of the bond. Other limitations on liability may be specified in special fields of CA records.²⁰⁹ The CAs have a duty to avoid conducting business so as to create a commercially unreasonable risk of loss to subscribers and persons relying on certificates.²¹⁰ The division enforces this and other duties, and it may seek injunctions and authorize private actions for violation of division orders.²¹¹

Subscribers that accept certificates from licensed CAs certify "to all who justifiably rely on the information contained in the certificate that . . . each digital signature affixed by means of the private key corresponding to the public key listed in the certificate is a legally valid signature of the subscriber, . . . [that] no unauthorized person has access to the private key," and that the information contained in the certificate is true.²¹² Such subscribers have a duty to exercise reasonable care in retaining control of their private keys and keeping them confidential.²¹³

Other jurisdictions should adopt measures like the Utah statute. In addition, applications must be developed that adapt public-key encryption to the particular needs of copyright owners and users. Standards for representing copyright information and for enforcing technological limitations on certain uses must be developed and accepted in the marketplace. No signs exist yet of any such widespread acceptance, and this limits the efficacy of encryption as a solution to intellectual-property concerns.

For encryption to become a significant part of the framework for protecting intellectual property, the law may need to impose duties not to compromise encryption. The *White Paper* proposes statutory language that would make it illegal to frustrate encryption and other copyright-management systems.²¹⁴

able under the circumstances.

Id § 46-3-401(5).

²⁰⁹ Id § 46-3-308 (establishing the effect of reliance limit; limitations on CA liability).

²¹⁰ Utah Code Ann § 46-3-207 (1995).

²¹¹ Id § 46-3-204.

²¹² Id § 46-3-302.

²¹³ Id § 46-3-303.

²¹⁴ See *White Paper*, Appendix 2, § 1201 (cited in note 5) (concerning circumvention of copyright-protection systems); id § 1202 (prohibiting false copyright information and removal of copyright-management information). There is precedent for this proposed legal duty not to compromise encryption schemes in the digital audio legislation. The passage

VI. FUTURE OF OPEN SYSTEMS

The risks of piracy may make content originators reluctant to publish their most valuable content in Internet-like architectures. In addition, the risks of no-fault liability may make intermediaries reluctant to handle valuable intellectual property in open architectures. The combination of these two forces may solve the intellectual-property protection problem by perpetuating arrangements that seem host-based, even though they are implemented in the World Wide Web or similar open network architectures.

The desire for certain features of closed systems does not doom the Internet model for the NII, however. For one thing, even if privately generated content is published only in relatively closed subparts of an overall open network architecture, the Internet and similar open network architectures will not die. Important parts of the world's information resources do not involve privately generated content. Public information is an obvious example. Intellectual-property protection is statutorily unavailable for federal-agency information, and should be unavailable for state and local public information.²¹⁵ The unavailability of copyright protection for public information may, on the one hand, encourage the deployment of closed systems to enhance the return to organizers of such information. However, an appropriate public commitment to make basic content available through the Internet on a nonexclusive basis, as required by the Paperwork

below compares the language of *White Paper* § 1201 with 17 USC § 1002(c)(1994), relating to digital audio recordings. Underlining indicates language in § 1201 not in § 1002(c); brackets indicate language in § 1002(c) not in § 1201:

1201. Circumvention of Copyright Protection Systems

No person shall import, manufacture or distribute any device, *product*, or *component incorporated into a device or product*, or offer or perform any service, the primary purpose or effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent, *without the authority of the copyright owner or the law*, any [program or circuit which implements in whole or in part, a system described in subsection (a)]*process, treatment, mechanism or system which prevents or inhibits the violation of any of the exclusive rights of the copyright owner under section 106*.

²¹⁵ See Henry H. Perritt, Jr., *Sources of Rights to Access Government Information*, 4 Wm & Mary Bill of Rights J 179 (1995) (cited in note 6) (marshalling legal arguments against copyright and copyright-like protection for public information); Henry H. Perritt, Jr., *Should Local Governments Sell Local Spatial Databases Through State Monopolies?*, 35 Jurimet J 449 (1995) (cited in note 6); Robert M. Gellman, *Twin Evils: Government Copyright and Copyright-Like Controls over Public Intermediaries*, 45 Syracuse L Rev 999 (1995) (cited in note 6).

Reduction Act of 1995,²¹⁶ should ensure against the locking up of public information and proprietary preserves. In addition, factual data are ineligible for copyright protection under *Feist v Rural Telephone Co.*,²¹⁷ but publishers have an economic interest in making such data available. Job-bank information is an obvious example.²¹⁸

Moreover, as the NII matures, the advantages of closed networks for protecting intellectual property and discouraging tortious and criminal content will lead to a merger of the open and closed architectures. While some role may remain for the original closed networks, like pre-1993 CompuServe, America Online, Westlaw, and Lexis, new Internet technologies likely will permit certain features of those approaches to exist alongside traditional open architectures in the Internet. For example, new tools are being developed to screen and block pornography in order to stave off federal legislation like the Exon amendment,²¹⁹ and they can be used to exclude persons who violate community rules. These tools would enable an Internet-based community to unplug someone, just as CompuServe or America Online may do now by canceling an account and password. Secure payment systems will supplement expulsion. These systems will deny access to certain Internet resources until appropriate payment arrangements have been made. This is possible now with a combination of Netscape CGI-bin scripts and public-key encryption. Access can be denied to a particular set of Web pages or newsgroups unless one has an account name and password associated with that particular set of resources. Public-key encryption permits private transmission of credit card numbers and authentication of an account holder's identity.

Suppliers of intellectual property will be drawn away from completely autonomous closed systems because of the flexibility of Internet-based tools like the Web and Netscape. In addition, the much larger potential market available through the Internet, compared to independent services that must convince people to subscribe, will attract supplies to public-key encryption as well.

²¹⁶ Pub L No 104-13, 109 Stat 163 (1995), codified at 44 USC §§ 3501-3520 (1995).

²¹⁷ 499 US 340, 345 (1991).

²¹⁸ See *Ink Plus Internet: Your 21st Century Recruiting Solution*, Int'l Herald Trib 6 (Aug 15, 1995) (advertisement for job marketplace for persons with advanced degrees at <http://chronicle.merit.edu>, or Gopher to: chronicle.merit.edu). For further information, contact Ink Plus at chronicle.com.

²¹⁹ S 314, 104th Cong, 1st Sess (Feb 1, 1995).

VII. FIRST AMENDMENT FRAMEWORK

First Amendment analysis is an important missing ingredient in the intermediary copyright-infringement cases. It is generally accepted that the fair-use defense internalizes First Amendment considerations into copyright law.²²⁰ However, courts that impose no-fault liability for copyright infringement on intermediaries²²¹ fail to consider the First Amendment at all. When courts impose no-fault liability on intermediaries for the information that they carry, the intermediaries are discouraged from certain activities. This results in a kind of de facto prior restraint.²²²

The First Amendment traditionally has been hostile to prior restraints, including governmental bans on publication before it occurs.²²³ Surprisingly, the constitutional preference for avoiding prior restraints does not operate when intellectual property is involved. "[N]o one denies that a newspaper can properly be enjoined from publishing the copyrighted works of another."²²⁴ The district court opinion in *New Era Publications International v Henry Holt & Co.*²²⁵ is an exception. In *New Era Publications*, a Church of Scientology affiliate brought suit to enjoin publication of a critical biography of L. Ron Hubbard, the founder of the Church of Scientology, on the ground that the biography infringed copyright. The district court found some infringement outside the scope of fair use, but nevertheless denied an injunction on First Amendment grounds. "[C]ourts should weigh cautiously whether a prior restraint in the form of an injunction is the appropriate remedy."²²⁶ The court also suggested that "[i]n determining questions of fair use and of remedy, [courts should consider] whether a copyright action is brought in good faith to preserve the benefits secured by the copyright law or whether it is brought to accomplish a different purpose, such as combatting

²²⁰ *Harper & Row Publishers, Inc. v Nation Enterprises*, 471 US 539, 549 (1985).

²²¹ See *Playboy Enterprises, Inc. v Frena*, 839 F Supp 1552 (MD Fla 1993).

²²² See *Cubby, Inc. v CompuServe, Inc.*, 776 F Supp 135, 139-40 (SD NY 1991) (stating that chilling effect of no-fault liability imposed on intermediaries leads to First Amendment limitations on standards for defamation liability for electronic-information intermediary). The same chilling effect occurs regardless of whether no-fault liability is imposed for defamatory messages or for intellectual-property infringement.

²²³ See *New York Times Co. v United States*, 403 US 713 (1971) (holding that enjoining publication of "Pentagon Papers" was impermissible prior restraint).

²²⁴ *Id* at 731 n 1 (White concurring).

²²⁵ 695 F Supp 1493 (SD NY 1988), *aff'd*, 873 F2d 576 (2d Cir 1989) (disagreeing with district court reasoning on First Amendment).

²²⁶ 695 F Supp at 1527.

a hostile or derogatory publication."²²⁷ More generally, the district judge noted that section 512 of the Copyright Act does not require courts to grant injunctive relief, and that "[w]e must, therefore, focus with new intensity on the potential conflict between the copyright and freedom of speech, and particularly on the question whether a finding of infringement should ritualistically call forth an injunction."²²⁸

The Second Circuit affirmed the denial of an injunction, but only on laches grounds. They disagreed with much of the district court's analysis, stating, "We are not persuaded, however, that any [F]irst [A]mendment concerns not accommodated by the Copyright Act are implicated in this action. Our observation that the fair use doctrine encompasses all claims of [F]irst [A]mendment in the copyright field . . . never has been repudiated."²²⁹ Chief Judge Oakes concurred, expressing greater support for the district court's analysis.²³⁰ Oakes recognized the strong authority against separate consideration of First Amendment matters in a copyright injunction, but nevertheless stated that judges have discretion to grant an injunction in a copyright case.²³¹ The matter did not rest there because the dissent from the denial of a rehearing en banc²³² urged that the panel majority opinion should not be understood as saying that injunctive relief follows as a matter of course once copyright infringement has been found. Rather, equitable discretion should determine the propriety of an injunction.²³³

A minority of the Supreme Court recognized that contractual restrictions also may offend the First Amendment by imposing de facto prior restraint, albeit in a case in which the United States government was a party to the contract.²³⁴ The dissent thus

²²⁷ Id at 1527 n 14.

²²⁸ Id at 1526 (characterizing 17 USC § 502 (1994)). A New York trial court also used an approach similar to that used by the district in *New Era Publications*. See *Rosemont Enterprises, Inc. v McGraw-Hill Book Co.*, 380 NYS2d 839, 843 (Sup Ct 1975) (denying injunction against allegedly infringing autobiography because injunction against publication would violate First Amendment).

²²⁹ *New Era Publications Intl v Henry Holt & Co.*, 873 F2d 576, 584 (2nd Cir 1989).

²³⁰ Id at 585 (Oakes concurring).

²³¹ Id at 596 (acknowledging that "[n]o Circuit that has considered the question . . . has ever held that the First Amendment provides a privilege in the copyright field distinct from the accommodation embodied in the 'fair use' doctrine").

²³² *New Era Publications Int'l v Henry Holt & Co.*, 884 F2d 659, 662 (2d Cir 1989) (on petition for rehearing and suggestion for rehearing en banc).

²³³ Id at 663-64.

²³⁴ *Snepp v United States*, 444 US 507, 516, 520 (1980) (Stevens dissent from majority holding that CIA agent who published memoirs in violation of CIA contract was subject to

supports the idea of a de facto prior restraint, but does not extend the concern into purely private activities.

The United States District Court for the Eastern District of Virginia recently ordered the seizure of the computer hardware and files of an Internet publisher who made copyrighted Church of Scientology text available.²³⁵ In another case, the District Court of Colorado issued an ex parte temporary restraining order ("TRO") and a seizure order, resulting in the seizure of computer equipment and software used by an Internet bulletin board.²³⁶ Twenty-one days later, the District Court denied a preliminary injunction, vacated most of the TRO, and ordered the return of the seized materials, commenting:

[S]uch relief [the requested injunction] would effectively pull the plug on Defendants' electronic library, infringe not only on their rights of criticism and research but be the death knell of FACTNET. . . . The injunction sought would silence the Defendants as participants in an ongoing debate involving matters of significant public controversy. Relief of this kind does not serve the public interest.²³⁷

Commentators agree that First Amendment and copyright interests should be balanced more explicitly. The law-review literature almost uniformly urges more attention to the First Amendment in copyright-injunction cases.²³⁸ This pressure from

constructive trust for all profits he made).

²³⁵ *Religious Technology Center v Lerma*, 897 F Supp 260 (ED Va 1995) (describing earlier temporary restraining order, order for impoundment, and writ of seizure directed at hardware for posting material on the Internet, but holding that First Amendment prevented injunction against the Washington Post).

²³⁶ *Religious Technology Center v F.A.C.T.Net, Inc.*, 901 F Supp 1519 (D Colo 1995).

²³⁷ *Id* at 1527. The district court in *Religious Technologies Center v. Netcom On-Line Communications Services, Inc.*, 907 F Supp 1361 (ND Cal 1995) appropriately considered First Amendment interests in rejecting no-fault liability for copyright infringement.

²³⁸ See Wendy J. Gordon, *A Property Right in Self Expression: Equality and Individualism in the Natural Law of Intellectual Property*, 102 Yale L J 1533, 1537 (1993) (cited in note 40) (noting that "legions of commentators have deplored" the tendency of courts to ignore First Amendment privileges when copyright or trademark suits are brought, but "the courts have too often turned a deaf ear to these arguments. The incantation 'property' seems sufficient to render free speech issues invisible."). See also Jessica Litman, *Copyright and Information Policy*, 55 L & Contemp Probs 185, 204 (1992) (questioning conventional wisdom that First Amendment need not be considered separately in copyright cases); Ralph S. Brown, *Civil Remedies for Intellectual Property Invasions: Themes and Variations*, 55 L & Contemp Probs 45 (1992) (surveying injunctive and damages remedies for intellectual-property invasion, and observing that injunction for copyright infringement is virtually automatic, despite plausible First Amendment concerns). See also

the literature likely will have some affect on the courts as copyright is used more aggressively to blunt NII activities.

Judicial willingness to grant injunctions is ironic, considering copyright's origins as a government-censorship tool.²³⁹ "Having a doctrine in free speech law that severely limits the use of prior restraints, only to throw it all out whenever even a small amount of someone else's expression has been incorporated into the defendant's speech makes no sense."²⁴⁰

Regardless of whether the copyright statute is involved, the courts should rediscover the First Amendment, follow the advice of commentators and the district court in *New Era Publications*; and recognize that copyright can be used to chill the kind of expression the First Amendment intends to shield. In particular, if intermediaries must censor unpopular views to avoid no-fault copyright liability, as some of the Church of Scientology cases suggest, First Amendment analysis should be used to apply fair use and ameliorate no-fault infringement-liability concepts.

Moreover, when ex parte seizure occurs, the victims should be able to object to the interference with their interests in an action on the bond under Rule 65 of the Federal Rules of Civil Procedure ("FRCP") and also in an action for damages under 42 USC section 1983. Persons who wrongfully obtain injunctive relief or otherwise use legal processes to interfere with another's property interests are subject to four kinds of sanctions: 1) damages against the bond required to be posted for interlocutory injunctive relief under FRCP 65; 2) damages for violation of civil rights under 42 USC section 1983;²⁴¹ 3) sanctions under special-

Comment, *Bare-Faced Mess: Fair Use and the First Amendment*, 70 Or L Rev 211 (1991) (urging evolution of fair-use doctrine to give First Amendment considerations more emphasis); Note, *Remedies for Copyright Infringement: Respecting the First Amendment*, 89 Colum L Rev 1940 (1989) (suggesting revised fair-use formula to accommodate First Amendment concerns better, including greater reliance on damages).

²³⁹ Diane Leenheer Zimmerman, *Information as Speech, Information as Goods: Some Thoughts on Marketplaces and the Bill of Rights*, 33 Wm & Mary L Rev 665, 677 (1992) (reviewing history of British copyright law and role of prior restraints not abolished until 1694).

²⁴⁰ Id at 737-738 (noting that if primary justification for protecting intellectual-property interest is economic, compensatory damages should be primary form of remedy).

²⁴¹ However, the victim of an ex parte seizure may have problems establishing state action. See *Wyatt v Cole*, 504 US 158 (1992) (holding that qualified immunity not available to private defendants in section 1983 actions for invoking state replevin, garnishment, or attachment statutes; remanding for determination whether state action was involved); *Jordan v Fox, Rothschild, O'Brien & Frankel*, 787 F Supp 471, 475-76, 480 (ED Pa 1992) (holding that attorneys executing confessed judgment were state actors and thus subject to liability under 42 USC § 1983, but also were entitled to qualified immunity as public officers). Most of the cases under section 1983 involve replevin or attachment, but

ized statutory provisions like that protecting against wrongful Lanham Act seizures;²⁴² and 4) common-law actions for abuse of process.²⁴³ Presently, however, the FRCP 65 solution often is not worth much,²⁴⁴ because the bonds are set very low,²⁴⁵ and the bond sets a ceiling on the amount that can be recovered by those wrongfully enjoined.²⁴⁶

VIII. INTERNATIONAL CONSIDERATIONS

The information superhighway is inherently international. Internet activities rarely respect national boundaries.²⁴⁷ A message sent from California goes as easily to an addressee in Israel as to one in California or Massachusetts. A client machine in Virginia can retrieve an infringing work located on a server in Sweden as easily as a client machine in Israel. Internet-like technologies usually permit the location of files and messages to be determined, and thus permit the location of an infringing activity to be located with reasonable certainty.²⁴⁸ However, detecting a violation in another country is not the same thing as realizing intellectual-property rights in an economic sense. Personal jurisdiction over the infringer still must be obtained, and a judgment or an injunction still must be enforced.

An effective property regime for the information infrastructure requires the development of appropriate doctrines to represent the balance between private ownership and public exploita-

the same reasoning applies to injunctions that affect interference with property interests.

²⁴² 15 USC § 1116(d)(11) (1994). See *Electronic Laboratory Supply Co., Inc. v Cullen*, 977 F2d 798, 804 (3d Cir 1992) (holding that attorney is not subject to sanctions under Lanham Act for wrongful ex parte seizure).

²⁴³ See Restatement (Second) of Torts § 682 (1965); *Wyatt*, 504 US 164 (discussing common-law malicious prosecution and abuse-of-process actions).

²⁴⁴ But see *qad. inc. v ALN Associates*, 781 F Supp 561, 562 (ND Ill 1992) (holding that bad-faith preliminary injunction in copyright case warranted increasing bond).

²⁴⁵ See *Religious Technology Center v F.A.C.T.NET*, 901 F Supp 1519 (D Colo 1995) (\$10,000 bond); *Religious Technology Center v Netcom On-Line Communication Services, Inc.*, 907 F Supp 1361 (ND Cal 1995) (\$25,000 bond); *First Technology Safety Systems, Inc. v Depinent*, 11 F3d 641 (6th Cir 1993) (setting \$2,000 bond for seizure of allegedly infringing articles rather than \$2.2 million requested by owner of seized articles).

²⁴⁶ But see *qad. inc.*, 781 F Supp at 562 (holding that bad-faith preliminary injunction in copyright case warranted increasing bond).

²⁴⁷ See Paul Edward Geller, *Intellectual Property in the Global Marketplace: Impact of TRIPS Dispute Settlements?*, 29 Intl Law 99, 101 (1995) (attacking widely accepted proposition that intellectual property is territorial).

²⁴⁸ Anonymous remailers are an exception to this general rule. Remailers are computers that strip electronic messages of all data identifying the sender and then deliver the messages wherever the sender wants. See Douglass Lavin, *As Regulators Seek to Police Internet, an Offbeat Finnish Service Fights Back*, Wall Street J (July 17, 1995).

tion of information. It also requires the development of international institutional arrangements that harmonize intellectual-property concepts²⁴⁹ and facilitate transnational enforcement.²⁵⁰

Recognition of the validity of the international character of markets for information and computer works stimulated efforts to append the Trade Related Intellectual Property ("TRIP") provisions to the Uruguay Round of the General Agreement on Tariffs and Trade ("GATT") negotiations.²⁵¹ TRIP largely incorporates the Berne Convention, which the United States signed in 1988.²⁵² The basic approach to copyright protection is to require "national treatment" to ban discrimination against foreign works,²⁵³ and to set minimum standards for protection.

Even if the principles expressed in TRIP are faithfully implemented around the world, however, additional work on adjudicatory and enforcement mechanisms is needed. Private international arbitration represents an attractive immediate means of simplifying choice of law and enforcement problems, inasmuch as the parties to an arbitration agreement can specify the law to be applied by the arbitrator. Most major trading partners have signed the international convention on the enforcement of international arbitration awards.²⁵⁴

An intellectual-property cooperative can play a useful role in developing a model arbitration agreement for handling transna-

²⁴⁹ See Geller, 29 Intl Law at 110-113 (suggesting that dispute-resolution panels established under the Trade Related Aspects of Intellectual Property ("TRIPS") might have the power to fill substantive gaps in protection) (cited in note 247).

²⁵⁰ The *White Paper* responds modestly to this need by proposing an amendment to 17 USC § 602 to include transmission in the definition of importation. United States Department of Commerce, Information Infrastructure Task Force, *Intellectual Property and the National Information Infrastructure: Report of the Working Group on Intellectual Property Rights* Appendix 1 § 2(c) at 98 (Sept 1995) ("*White Paper*") (cited in note 5). The *White Paper* notes that "[b]ecause copyright laws are territorial, and the standards of protection embodied in the international conventions leave room for national legislative determinations, acts that may constitute infringement in one country may not be an infringement in another country." Id at 118.

²⁵¹ *General Agreement on Tariffs and Trade: Agreement on Trade-Related Aspects of Intellectual Property Rights*, 33 ILM 81 (1994).

²⁵² J. H. Reichman, *Universal Minimum Standards of Intellectual Property Protection Under the TRIPS Component of the WTO Agreement*, 29 Intl Law 345, 370 (1995) (TRIP adopts a "Berne plus" approach); Berne Convention Implementation Act of 1988, Pub L No 100-568, 102 Stat 2853 (1988).

²⁵³ See *Creative Technology, Ltd. v Aztech System PTE, Ltd.*, 61 F3d 696, 700-701 (9th Cir 1995) (describing national treatment and dismissing on forum non conveniens grounds copyright-infringement suit brought by Singapore plaintiff).

²⁵⁴ 1958 United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards ("New York Convention").

tional intellectual-property problems in the information infrastructure. In the long run, such cooperatives also can be forums within which other private international-law initiatives can be crystallized.

CONCLUSION

New information technologies disrupt historic balances between the competing interests involved in intellectual property. However, owners of intellectual property should not be granted enlarged economic protection merely because they would like it. Protecting intellectual property in a flourishing NII depends more on the imagination of entrepreneurs in designing and deploying new business and pricing models, and depends less on legal creativity.

The Administration's *White Paper* does not make a strong case for amending the copyright law. A preliminary analysis of the relative costs of originators and pirates in new electronic-publishing environments such as the World Wide Web suggests that new product design, new business methods, and new technology protections can more than make up for increased risks of piracy due to reduced copying costs. Congress should reject the recommendations of the *White Paper* and leave the present copyright statute intact. On the other hand, if the statute is amended, statutory protection for intermediaries may be appropriate. A safe harbor for caching and stronger protections against ex parte seizure orders may be appropriate. Regardless of whether the copyright statute is amended, courts applying the statute should rediscover the First Amendment.

A combination of existing intellectual property and contract protections are sufficient to prevent gross piracy, especially when reinforced by anticipated changes in pricing and new product concepts and packaging. Copyright cooperatives can play a useful role in reducing transaction costs for new types of protection based on technological limitations on unauthorized uses, technological detection of copyright and license violations, and electronic payment systems. In addition, cooperatives can express and enforce specific-use licenses and can address international issues relating to choice of law and enforcement of judgments.

Figure 1

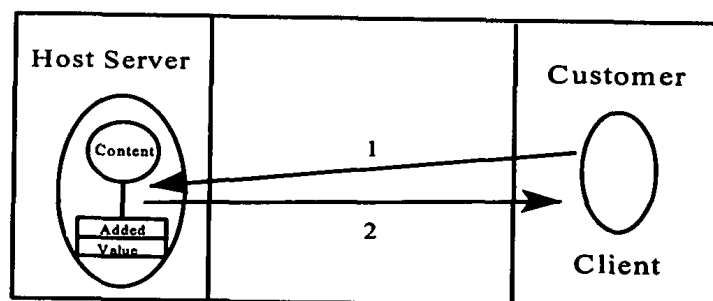


Figure 2

Internet as a Market for Disaggregating Value Production

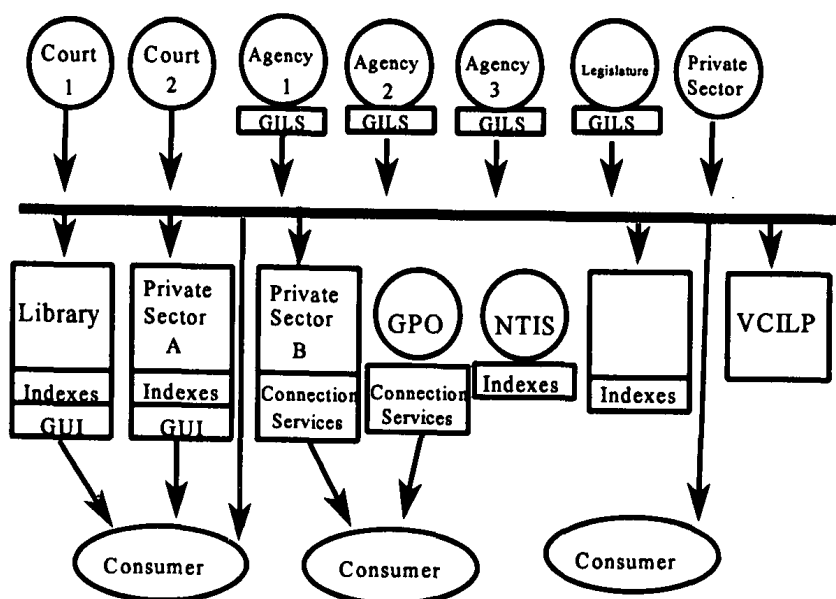


Figure 3

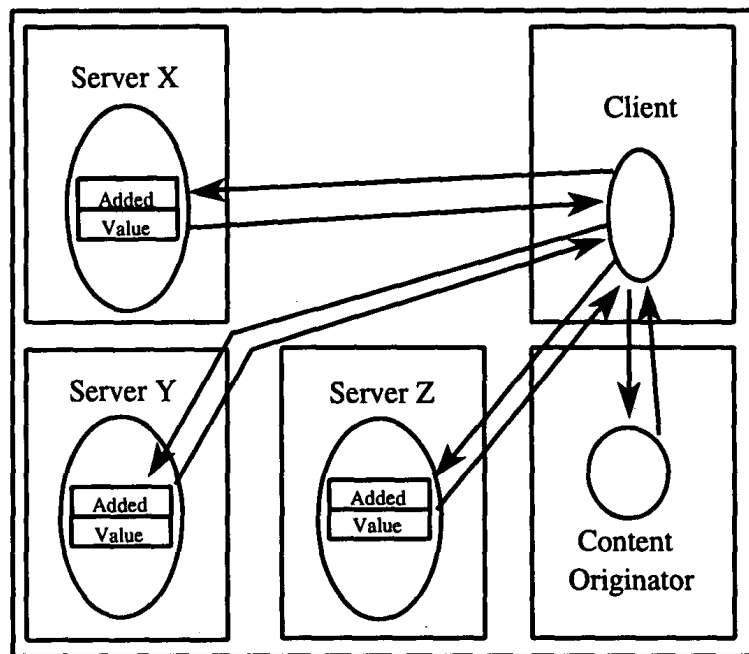


Figure Four

TECHNIQUE	ANALOGY	ELECTRONIC EXAMPLE
1. Planned obsolescence	Supplemented professional books	frequent updates of material
2. Finer granularity		Small HTTP or gopher retrievable files
3. Addition of presentation markup		HTML tagging
4. Bundling vulnerable material to less vulnerable value-added elements		Embedding content in CD-ROM software; WESTLAW and LEXIS
5. Concentrating investment on value-added features other than content		Web server subsidizes suppliers of content on other servers
6. Subsidies of content producers by producers of downstream value	Collective licensing schemes	
7. "Global" license for creator in exchange for share of revenues determined per some aggregate formula	Advertising	
8. Third-party subsidy	Newspaper	
9. Giving content away to attract customers to electronic markets		WESTLAW, LEXIS passwords
10. System access controls		CNI/Library of Congress test bed
11. Content encryption		
12. Extremely low transaction-cost payment systems linked with chunks that are not worthwhile to steal		