Richmond Journal of Law and Technology

Volume 6 | Issue 4 Article 4

2000

The Developing Legal Infrastructure and the Globalization of Information: Constructing a Framework for Critical Choices in the New Millennium Internet -- Character, Content and Confusion

Tomas A. Lipinski

Richmond Journa l of Law &Technology

Volume VI, Issue 4, Winter 1999-2000

The Developing Legal Infrastructure and the Globalization of Information: Constructing a Framework for Critical Choices in the New Millennium Internet -- Character, Content and Confusion

by: Tomas A. Lipinski [*]

Cite As: Tomas A. Lipinski, *The Developing Legal Infrastructure and the Globalization of Information: Constructing a Framework for Critical Choices in the New Millenium Internet -- Character, Content and Confusion*, 6 RICH. J.L. & TECH 19 (Winter 1999-2000) <http://www.richmond.edu/jolt/v6i4/article2.html>. [**]

Table of Contents:

I. INTRODUCTION

{1} This paper [1] reviews recent attempts to extend traditional property rights and other information controls and regulations into new media, such as cyberspace, primarily the World Wide Web. It reviews developments in copyright, trademark, trademark dilution, misappropriation, trespass, censorship, tort, privacy and other legal doctrines as they are reflected in recent United States case law and legislation, and to a lesser extent, in international agreements. Legal problems often arise because there is a conflict of viewpoints in how to best characterize space on the Internet, specifically the World Wide Web. Some argue that traditional ownership rights should apply, or perhaps a model of limited property rights, which assumes an implied license to "trespass" or move within that space, *e.g.*, to visit or to link to another website. Others believe that private ordering systems, like contract law, should dominate the negotiation of information boundaries. Still, others see the Internet as the "last open frontier," or at least, as the "last green space" or "commons." This debate is assessed in light of several implications for information in the new millennium, *i.e.*,the post-national era, as it is naive to assume that simply because borders may dissolve or boundaries may expand through technology, that information access and equity will also naturally increase.

{2} Initially, definitions of several terms, such as harmonization, globalization, and a suggested alternative, amelioration, are offered not to portray an information Armageddon, but to point out the dangerous potential of new trends in information ownership and control. A significant portion of the discussion herein reviews recent legal developments in information ownership and control, and characterizes these developments into several themes: iteration, redaction, reaction, and marginalization. Examples of iteration demonstrate that traditional information boundaries are breaking down. In its place, redaction occurs as new concepts of information ownership and control succeed. In reaction to this, many sovereign states and entities are adopting self-protection measures to protect their information resources. Finally, marginalization occurs when alternative concepts of information access and control are discounted in the name of universal progress, and so the interests of many information users become outcast or otherwise ignored.

{3} The article concludes with a review of several myths that are often forwarded in the debate against those who attempt to regulate, through law, conduct in cyberspace. The myths are not so much rebutted with alternative maxims, but questioned in the hopes of forwarding an understanding of why these legal controversies have developed, and will continue to develop in cyberspace, as well as their impact upon world citizens in the post-national era. The first myth is a general statement that conduct and content cannot be regulated on the Internet through law because the Internet is an open system, with no boundaries, and thus, laws cannot practically apply. Another myth is that the best characterization of the Internet is that of "last frontier." Taken to its extreme, this position advocates a certain "information vigilantism." Perhaps less overt, but pernicious nonetheless, is the increase in the number of advocates for self-normative regulation of the Internet. In reality, this option envisions a series of private rights as the dominant mode of information access vis-à-vis the freedom to contract. The concept of the Internet as the new "green space," akin to a virtual commons is critiqued. In contrast, the reality of recent World Wide Web litigation suggests that legal

institutions are adopting existing concepts and nomenclature to the information problems of virtual spaces, *i.e.*, "cybertort" and "cyber squatter." For better or worse, the law is adapting the legal ordering of its ownership and control schemes to cyberspace and the "fencing" of boundaries in cyberspace continues.

A. *Harmonization*

{4} The first concept, harmonization, is a familiar one. Harmonization is a term used most often to describe the process of conforming national laws to some basic international standard. An example is the impact of the recent WIPO ("World Intellectual Property Organization") treaties. [2] These treaties were negotiated to protect copyrighted material in digital environments and to provide stronger international protection to performers and producers of sound recordings. In the United States, these developments resulted in the recent passage of the Digital Millennium Copyright Act of 1998. [3] Harmonization is a mechanism of fairness, as it ensures that similar acts in different places (*i.e.*,signatory countries) will produce similar results. In the case of the copyright example, it means that a work will be protected in all countries that agree to abide by the terms of the treaty. [4] Harmonization is also efficient, in that it eliminates the transaction cost of negotiating agreements between information sellers and information buyers in every location where, in the case of copyright for example, the work would be available for sale. In this manner, harmonization also facilitates access, as some producers may be reluctant to offer their information products and services to the citizens of particular countries where such protections are not in place.

{5} Harmonization relates to the information infrastructure under which such a country may be forced to operate. It is in this way, that harmonization exhibits its more detrimental side. Harmonization is in essence a lowest common denominator approach to information access and control. It is characterized by the internalization of external standards. While this may not be negative in and of itself, questions of equity arise when the decision-makers, or those who set the external standards are primarily First World countries, who are considered the "information rich" and the decision-takers (*i.e.*,Third World countries), known as the "information poor" are not. It should also be observed that this disparity could, of course, exist within the borders of a sovereign state as well. Problems can also arise within a particular country when the national or commercial interests of a segment of the population supercede the collective access rights of its citizens. An example of this is occurring with the attempts to harmonize United States law with the European Community Data Protection Directive 96/9/EC, [5] which was enacted in March 1996 to protect online and real time databases throughout Europe. [6]

{6} As a result, successive congresses have attempted to pass a similar protective law for databases in the United States. [7] If the legislation is passed, the ability for subsequent users to incorporate portions of pre-existing databases will lessen, even when the content of the database would otherwise be in the public domain (*i.e.*,it is factual or otherwise contains uncopyrightable material). This creates a new *sui generis* protection for basic information beyond the existing copyright and misappropriation law. [8] Instead of protecting originality, the bill, if enacted, would protect an information owner's investment in organizing, assembling, and maintaining information, and in essence, reverses the decision of the United States Supreme Court. [9] This is figuratively known as the owner's "sweat of the brow." By its design, the bill rewards the economies of scale that existing information owners and developers draw upon. [10] This may work to stifle competition from start-up and smaller existing companies and it will ultimately make information less available, as it subjects the information to stronger protection regimes and makes new database development more costly for new entrants. In addition, the "fair use" provisions for schools, libraries and other non-profit enterprises contained in one of the proposed pieces of legislation are inadequate. [11]

{7} Finally, harmonization, as applied in past scenarios ignores the individual uniqueness of certain markets in the name of inter-operability. In this manner, harmonization can be said to offer a debasement of information concepts or integrity. A country may, within its boundaries, have indigenous property systems

that are communal in nature or based upon some other concepts that stand in opposition to copyright. In order to attract foreign investment that country may agree to harmonize its own laws according to the developing international order. [12] As a result, the country may diminish its own information heritage or disenfranchise a portion of its own constituency. This results in a debasement of the cultural information heritage of a country in the name of economic progress.

B. *Globalization*

{8} The second term - globalization - is also familiar. Globalization refers to the natural trend in information access and control that is developing through market factors. In the new millennium, the dominant good or service will certainly be information-based. [13] When assessing the trend in the globalization of the Internet, primarily the World Wide Web, or the development of information products and services in traditional spheres in recent years, one cannot help but be struck by the growing commodification of information. [14] The commodification of information results in a globalization process whereby policy decisions involving the right to control information, and the right to access that information are based solely upon the marketplace. This commodification trend will be further discussed in a subsequent section of this article.

{9} Globalization does not, by its definition, limit its application to a market model. However, the reality facing the interrelationships among sovereign states and actors within those states with other states and states' actors is such that, the basis of those relationships is tied to the infiltration of commercial interests and the dominance of market factors, to the exclusion of other principles. [15] Under this model, decisions concerning information access and control are based primarily upon economic factors. [16] A decision, for example, of an international media conglomerate to invest in a developing country is based not upon a concern for the information needs or equity of that country's citizens. Rather, the decision is based upon whether or not demand exists for the conglomerate's information product or service in that country and whether the conglomerate could successfully meet and profit from that demand. [17] As a result, "[w]hile some societies will be able to share some of the benefits of economic growth and welfare resulting from globalisation [sic] others remain excluded and increasingly marginalized." [18] Further, what about the marginalization of particular groups within a country that is generally advancing? This is a problem even within the United States, for example, with the development of the concept of universal service in new telecommunications settings. [19] Globalization is often characterized by the domination of external economic forces upon another country.

{10} It takes time for a lesser-advantaged country to develop its markets. Consider the case of India or China. For years, both countries were leading sources of copyright infringement of United States' information products and services, especially computer programs. [20] India and China were also reluctant to join any international copyright agreements. When India's and more recently - and to a lesser extent - China's own intellectual property markets developed, and then other less-advantaged countries, in turn, pirated their works, both countries became more concerned with supporting stricter international copyright enforcement. [21] This enforcement would better position each country's information products and services in the global marketplace. However, countries like India and China will have to continually weigh the cost of international copyright enforcement among their own populations with the incentives of domestic productivity, international investment, and possible dissolution of traditional views of property that may be inherent in their cultures. [22]

{11} The implications of this domination are important if various commentators [23] are correct in their assessment that intellectual property and information will become the currency of the Twenty-First Century. Thus, those countries that have established intellectual property infrastructures will be at an advantage to dominate internat'l markets. The national governments of sovereign states or multi-states will increasingly play a role in designing protection measures for their own constituents, and if the direction of that protection

is in response to external forces, then a country's national information policy may become incongruent with the needs of its own people. This can result in a commodification of culture. [24] The critical policy question involves achieving the proper balance between establishing a climate of property-oriented incentives to encourage information infrastructure investment and the rapid diffusion of technology, on the one hand, and the provision of this investment climate at the possible exclusion of the public interest on the other. [25] In an information marketplace geared towards globalization, achieving this balance becomes more difficult.

{12} Consequently, it should come as no surprise that, "[t]he digital revolution is good news for everyone in the business of protecting intellectual property. As ideas and knowledge assume a larger part of the nation's wealth and international trade, intellectual property protectors will become increasingly important to the country's future." [26] Moreover, these primary players will likely be able to determine what the rules will be for subsequent international players and their respective transactions. Like the industrial capital of the Eighteenth and Nineteenth Centuries, intellectual property and other information rights, such as the control of the content of speech will become the "raw goods" and "working capital" of the new millennium. As a result, those who have control over that information are placed in superior positions for the purposes of subsequent information transfer and development. [27]

C. *Amelioration*

{13} The alternative to the above approaches is the concept of amelioration. This is perhaps a new concept, but it does have its roots in the hopes originally placed upon the preceding concept of globalization. Amelioration recognizes the connected and interrelated nature of the post-national era: the dissolution of traditional boundaries (in the climate of existing globalization, this is perceived as a ***negative*** concept), but also the potential for the structuring of new ones (in contrast, amelioration is seen as a ***positive*** concept). Amelioration also recognizes the concept of harmonization that must occur naturally if the holders of diverse interests are to find common ground upon which to build new relationships. However, amelioration is a positive concept that envisions international intellectual property agreements, [28] or international commercial development, [29] for example, that attempt to retain the intrinsic uniqueness of each sovereign state, rather than to dismiss or to usurp that as primitive or otherwise unworthy.

{14} Whether mechanisms such as Pareto optimization or Rawlsian distributive justicen [30] can be incorporated into existing international agreements remains to be seen. Consider the concept of economic justice as applied to amelioration. Two alternative models of decision-making may be considered: Pareto optimization and a Rawlsian notion of distributive justice (as based upon the work of John Rawls). Consider the case of a country considering accession to an international agreement that would open its information markets to foreign investment and development. A Pareto optimum approach to harmonization or globalization would hold that no law, international treaty, or agreement should be adopted by a country, nor its markets opened to foreign influence, unless all of the parties are no worse off by the activity and the position of at least one party improves because of the action. Rawls would suggest that adoption or implementation occur only if the least advantaged (namely, the developing country) is placed in a better position as a result of the development of the information market infrastructure vis-à-vis the harmonized law or globalization investment. Amelioration dictates that at least a Pareto optimum approach is taken, such that no party, including the developing country is disadvantaged. Further, amelioration favors a Rawlsian approach, as it is one in which the developing country is advantaged. In the current climate of harmonization dominated by First World property interests, and globalization dominated by First World market interests, neither occurs. As observed earlier, the developing, less-advantaged country is often left in a worse position.

{15} Arguably, these concerns were part of the original intent of concepts like harmonization and globalization, but were quickly superceded as political and market forces dominated international relations. The implementation of the amelioration concept remains a challenge for future commentators.

II. Trends In Information Ownership And Control In The Post-National Era

{16} In assessing the development of legal responses to information ownership and control, several themes or trends emerge. These themes or trends attempt to categorize the "fall-out" from the harmonization/commodification/globalization juggernaut. Identification and assessment of these trends is the initial phase of the global policymaking activity. These themes place the recent information warfare disputes into one of four models: iteration, redaction, reaction, and marginalization. While specific solutions are not forwarded, the identification of these developments is helpful to subsequent commentators when formulating and designing appropriate national and international policy responses. Once identified, these patterns may be more keenly monitored and assessed within a country's policymaking processes, as well as within a broader global policymaking agenda in order to minimize possible negative effects. The balance between information owners with control rights and information users with access rights is dynamic. As harmonization and globalization move forward, realignment often occurs. The re-adjustment often provides the opportunity for the ascension of control rights as an incentive to development, but at the expense of access rights, which in the long run, may hamper development. Having the observation tools to assist in the monitoring of these developments may help thwart unwanted effects of these processes.

A. *The Decline of Traditional Information Boundaries: Information Iteration*

{17} The emergence of new information technologies, such as the Internet and the World Wide Web forces traditional legal concepts of information to be adapted to these new environments. As a result, there is a breakdown in traditional information boundaries. Iteration occurs when existing legal concepts are applied with less than convincing results to web environments. The law attempts to place new or unknown circumstances into known or existing categorizations or characterizations. When the match results in analogies that are clumsy or intuitively unsound the integrity of the law - as an arbiter of information control and access disputes - is questioned. As a result, there is a breakdown of the traditional information boundaries.

{18} Two examples can be used to demonstrate this principle. Consider the application of the concepts of free speech and copyright to the World Wide Web. Courts have tried to describe virtual space in terms that are familiar, though less than precise. In a case involving the constitutionality of a law designed to regulate content on the Internet, the United States Supreme Court stated that, "[t]he Web is thus comparable, from the reader's viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services." [31] A subsequent lower federal court attempted to apply the "Internet as a library" analogy in characterizing the use of a software filter to censor content in a public library as similar to a "book removal," thus making it subject to strict scrutiny under First Amendment jurisprudence. [32] The use of the software filter was found to be unconstitutional. As the federal court stated:

> After considering both arguments, we conclude that defendants have misconstrued the nature of the Internet. By purchasing Internet access, each Loudoun library has made all Internet publications instantly accessible to its patrons . . . In effect, by purchasing one such publication, the library has purchased them all. The Internet therefore more closely resembles the plaintiff's analogy of a collection of encyclopedias from which defendants have laboriously redacted portions deemed unfit for library patrons. [33]

{19} The problem is that, while both decisions represent victories for free speech advocates, the analogy used by courts thus far does not seem to comport with how library collections are actually built and constructed by library professionals. [34] These judicial analogies and characterizations are ill-suited to emerging technological media.

{20} Likewise, courts have struggled to apply traditional "photocopying" scenarios to Internet copying and browsing with less than convincing articulation. One court decided that an online service provider was not responsible for the postings of others on its system. A federal district court reasoned

> 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 pubic make copies with it. 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. [35]

{21} Later, the court also observed that browsing was allowed in digital environments, even though as a precursor to the viewer's act of reading or observing the image on the screen, a "copy" is made that resides in the computer's RAM. The court concluded:

> It [browsing] is the functional equivalent of reading, which does not implicate the copyright laws and may be done by anyone in a library without the permission of the copyright owner. However, it can be argued that the effects of digital browsing are different because millions can browse a single copy of a work in cyberspace, while only one can read a library's copy at a time. [36]

{22} This difficulty of applying copyright concepts from the analog world to the digital world has not escaped comment by scholars. [37] If courts cannot adequately characterize new information disputes with consistency, the digital environment may threaten existing legal mechanisms of information order altogether. For example, several commentators predict that copyright will cease to exist as a mechanism for ordering rights between owners and users. [38] This is due primarily to the high transaction costs associated with the use of copyrighted materials in digital environments. Users have the ability to make perfect copies with great speed and to distribute the copies to multiple users with as much ease. [39] Likewise, copyright owners have little ability to track or control impermissible uses. [40] In its place, many commentators see the rise of alternative legal doctrines that were never intended to apply to copyright-like information. [41] One example is the misappropriation doctrine. This doctrine is reflected in the NBA game pager litigation in which the Second Circuit articulated a "hot news" exception for the use of real-time event information. [42] Misappropriation was also one of the claims in a recent web-link dispute. [43] However, that case is indicative of the types of suits likely to arise as information owners seek new legal mechanisms to control their interests. Originally designed to remedy "takings" in a commercial setting, misappropriation is ill-suited for situations were public rights, such as fair use and access rights to basic factual information are involved.

{23} Another recent development is the rise in private contracts to negotiate ownership and use rights between parties. This can be seen in the recent discussions concerning the revision of the Uniform Commercial Code ("U.C.C.") and the proposed Uniform Computer Information Transactions Act ("UCITA") which would make information a "good" subject to contract terms, just like any other good. [44] This trend is also evidenced in the proliferation of shrink-wrap licenses, and web-wrap licenses now in use. These licenses have received judicial imprimatur from the Seventh Circuit when it validated the use of such mechanisms to protect otherwise uncopyrightable information. [45] The facts of that case are instructive of the dangerous effects that an iterative information environment may have on information access. The defendant, Zeidenberg, purchased a ProCD CD-ROM of telephone subscriber information, and in keeping with existing copyright law, extracted the unprotected names, addresses, and telephone numbers, created his own search software, and loaded the contents onto the Internet much to the chagrin of ProCD. At the district court level, Judge Crabb, relying on previous law, [46] ruled in favor of Zeidenberg. [47]

{24} On appeal, the Seventh Circuit rejected every point of the district court opinion. For example, the validity of the shrink-wrap license was upheld because "Zeidenberg inspected the package, tried out the software, learned of the license, and did not reject the goods." [48] The most important point made by Judge

Easterbrook is that a user of copyrighted material may bargain away his copyright fair use right or other "use" privileges if that user or consumer chooses to do so. [49] For example, another such use right is the first sale doctrine, which allows a purchaser of copyrighted material to dispose, through gift or resale, of the copyrighted material. The right of control over the work by the copyright holder ends after the first sale of that work to any given consumer. The Seventh Circuit decision explicitly permits a publisher to protect uncopyrightable information by private contract. [50] This information would otherwise be available for reuse or republishing under fair use or other provisions, such as the first sale doctrine of the copyright law. The court also validated the use of shrink-wrap license to protect software and the validity of web-wrap and click-on licenses.

{25} The result highlighted from case law such as that raised in the Seventh Circuit is the emergence of a normative Internet regime based upon private contract. Commentators have been critical of reliance on private ordering on the Internet. [51] Allowing the rights of information users to be determined solely by contract will generally benefit only those parties that have the power, in terms of bargaining and parity of contract, to negotiate. Most individual users, such as Zeidenberg, are simply not in a fortunate position from which to bargain.

{26} Traditional legal concepts are also difficult to apply when assessing commercial activity on the World Wide Web. The problems arise in those circumstances where a formal contract does not exist, but some other level of interaction between the parties does exist. This interaction must rise to a level of sufficient contacts with the forum state and the cause of action to satisfy the "minimum contacts test" set forth by the Supreme Court. [52] However, the law is far from well-settled in the more complex and ambiguous situations, such that, "[i]n cases in which a defendant's electronic contact with a foreign jurisdiction is based on a Web site that is accessed in that jurisdiction and not accompanied by a contractual relationship, courts have reached disparate conclusions." [53] Courts consider what level of activity must occur in a commercial website setting between the owner or proprietor in one jurisdiction, and a customer in another jurisdiction, before concluding that the owner-proprietor was "doing business in" or otherwise engaged in sufficient minimum contact. [54] Jurisdiction can be either general, if it is the result of continuous and systematic contacts, or specific, when resulting from the website owner-proprietor's contacts with the forum.

{27} In the real world, when a customer walks into a store, the jurisdiction (*i.e.*, general jurisdiction) is established by the store's physical presence and its daily activity that is substantial or continuous and systematic. How does this concept apply when the store exists in cyberspace? Virtual courts do not exist, therefore the practical matter of which forum should settle the dispute still needs resolution among the parties to the litigation. The customer would like to litigate the case for most practical purposes in his home jurisdiction. For better or for worse, this same logic -- presence of store or a commercial site establishes general jurisdiction -- does translate to the Internet. What about the minimum contacts necessary to establish specific jurisdiction?

{28} Most courts have held that mere presence on the World Wide Web is not sufficient to establish jurisdiction. [55] However, in *Bochan v. La Fontaine*, [56] the court concluded that, since a Texas Usenet member's posting must, at some point, be stored on America Online's server in Virginia, jurisdiction existed in the latter state. One commentator recently speculated on the unpredictability of judicial responses to jurisdiction in the online realm: "Bochan is viewed widely as an aberration, but it does show that courts still can throw curves in an arena in which the law and technology are changing rapidly, and of which judges have divergent perceptions." [57] If the website owner-proprietor physically resides in another jurisdiction, then extending the customer's home jurisdiction over the personage of the website owner should occur on some reasonable legal basis. Some courts have looked to the amount of inter-activity that the web site allows its customers to engage in while visiting the site, establishing a sort of sliding scale of Internet-based contacts. [58]

{29} Generally, a mere web presence is not enough, *i.e.*, just because a customer can access a web site from his jurisdiction, that jurisdiction should have forum rights over the website owner. However, the Securities and Exchange Commission ("SEC") has held that a mere hyperlink, providing "direct access" from one site to another associates the two as a single electronic document for purposes of the insider trading laws. [59] But, should the mere ability to access or to link to a site from one jurisdiction be tantamount to a "presence" for purposes of exerting the potential of legal remedy, *i.e.*, the establishment of the minimum contacts of specific jurisdiction? The problem is exacerbated when one considers the international ramifications of making these policy decisions. Consider the following case in point: the Georgia Institute of Technology needed to defend itself in a French court because its website was not also available in French, and thus, violated the French law requiring use of the French language. The case was dismissed, but not until after the initial complaint was filed and the defendant answered. Furthermore, the dismissal was not based upon the lack of jurisdiction. [60]

{30} A final example is found the inability of trademark law to adequately adapt to web environments. This occurs because principles of federal trademark registration, for example, allow for similar or identical trademarks in differing product or geographic markets. [61] Similar or identical marks may coexist as long as there is no consumer confusion. [62] Unfortunately, this concept is not easily translatable to the World Wide Web. Thus, the use of domain name information is less freely available in the digital environment. [63] This occurs because, while there may be a Lexus automobile manufacturer and a LEXIS-NEXIS online database, or a Beretta automobile and a Beretta firearm, there can only be one entity with the domain name "beretta.com." [64] In the physical non-digital world, use of the word "Beretta" by each company is possible under trademark law. [65] This is a practical impossibility in the digital world, as there can be only one "beretta.com" domain name. [66]

{31} Another interesting development results when individuals try to exploit the limitations of domain name assignment technology. F. Lawrence Street observes that, similar to other limited commodities, competition for domain names motivates parties to reserve certain domain names in hopes of later selling that name to the owner of the trademark with the same name. [67] To a commercial entity, a domain name, like a trademark, has great value. [68] This has led to the development of a futures market for domain names with savvy individuals staking claims to numerous domain names, in the hopes of later selling the registration to wealthy corporations. [69] Companies have become incensed upon discovery that someone has reserved the obvious or likely domain name for their company's product or service. In fact, the law has developed a name for these domain name usurpers: "cybersquatters." [70] Dennis Toeppen, has, at one time or another, been the owner of over 200 different domain names, including "deltaairlines.com," "britishairways.com," "northwestairlines.com," "ramadainn.com," "eddiebauer.com," and "neiman-marcus.com." [71] In *Avery Dennison Corp. v Sumpton*, [72] Free View Listings, another cybersquatter, registered over 12,000 surnames as domain names. [73] Not surprisingly, Toeppen and other cybersquatters have been successfully sued on trademark infringement or trademark dilution claims. [74]

{32} One way for a company that believes its cybermark has been misappropriated to protest the transaction is to file a petition with Network Solutions, Inc. ("NSI"), the organization that administers the domain name system. [75] Challengers choose the NSI forum because the overwhelming number of disputes are resolved by NSI in favor of the challengers. [76] In cases of true cybersquatting, this may be the correct result, but many other trademark holders have abused the system, taking advantage of the NSI policy and moving against legitimate cyber domain name registrants. [77] This abuse of the system dedicated to curbing the misappropriation of domain names has led some to comment that, "[t]hese cases illustrate what has come to be a practice known as reverse domain name hijacking." [78] The NSI policy is perhaps indicative of the general reaction to the new "cyber space," the breakdown of traditional rules of property.

{33} Global responses are also developing. [79] The recent WIPO Final Report of the WIPO Internet Domain Name Process (the "WIPO Report") [80] details procedures for resolution in situations of abusive registrations and famous mark only. However, the WIPO Report does not offer alternatives to the simple fact

that, while commercial entities may operate with similar trademarks without violating the principles of the trademark law, there can be only one owner of a domain name with the .com gTLD. This problem is further complicated by the fact that there are a limited number of unrestricted gTLDs (.com, .net, and .org).

{34} As traditional information boundaries are stretched to adapt to the new legal challenges of the Internet, the existing information order breaks down. Information owners and users are no longer sure of their responsibilities and opportunities with respect to the use of information. Iteration occurs, in which the law attempts, often with inconsistent or inadequate results, to arbitrate between opposing parties, as is the normal function of the law. New meta-information boundaries have arisen, which offer the potential for a further loss of public rights in information. These are described in more detail in the following section.

B. *Ascension of New Meta-Information Boundaries: Information Redaction*

{35} Redaction in the legal infrastructure supporting the information environment occurs when new barriers or boundaries are created that may impact upon a state's or individual's access to, or use of information. This redaction can be international in scope or it can occur within a sovereign state. The earlier section of this article discussing the emerging concepts of harmonization and globalization recounted the developments involving trends in international copyright and *sui generis* protection for collections of information, *e.g.*, databases. Here, two additional examples serve to illustrate the specific point of redaction. Redaction is often a legal response to the "newness" of the Internet as a medium. Current legal "solutions" to so-called information harms or wrongs are edited or redacted, to commit principles that, in the analog world, would simply not apply or extend.

{36} Consider the recent attempts to regulate the content of Internet communications in the United States. [81] Laws have been drafted to protect users from unsavory content. The Communications Decency Act of 1996 ("CDA"), part of the Telecommunications Act of 1996, [82] was designed to protect minors from indecent transmissions and patently offensive displays. The problem was that the statute, as enacted, effectively prevented anyone from sending or displaying indecent or patently offensive material. A community organization that posted on its website sexually explicit material, targeted at preventing unwanted pregnancy or sexually-transmitted diseases among teenagers might be guilty of a felony. Likewise, high school students who e-mailed each other about their "sexual experiences" might also face prosecution. [83] As noted earlier, the Supreme Court struck down the law as unconstitutional. [84] In its place, however, Congress passed the Child Online Protection Act of 1998 ("COPA"), [85] but the new law was euphemistically referred to as the "CDA II" or the "baby CDA." While, the new law purported to restrict the availability of materials to minors, the effect of the law was to restrict adults from communicating and receiving expression that is otherwise protected under the First Amendment. The law targeted the commercial providers of information by imposing a series of checks that would force content providers to censor themselves or simply to withdraw from the Internet medium. The law is under current court challenge. [86] Both statutes are examples of legal restrictions forwarded by legislatures that not only extend the reach of the law into cyberspace, but also extend that reach beyond what was normally thought to be the conforming limits of the law. [87] In response to the "newness" of the Internet environment, legislatures often see fit to regulate conduct beyond that which can be proscribed in an analog or print-based setting.

{37} Another example of sweeping legal reform in cyberspace also derives its origin from the Telecommunications Act of 1996, the Online Family Empowerment provision of the CDA. [88] This provision remains in effect today, as it was not part of the previous constitutional challenge. The current version of 47 U.S.C. §230(c) creates a "good samaritan" provision that was originally drafted to protect providers of an "interactive computer service" from tort liability, when attempts to prevent defamatory postings on their bulletin board services are unsuccessful. Developing case law held the provider responsible for postings made by third parties when the provider made assertions that it would protect users from such

rogue postings. [89] The law was, in part, a response to the burgeoning cybertort litigation that, if unchecked, was perceived to have the potential to dampen free discourse in bulletin boards, chat rooms, and other asynchronous communication technologies. Congress wanted to remedy this scenario and to reward online service providers with tort immunity for their attempts. [90] This amounted to sweeping legislation, as courts have begun to apply the new law not only in cases of defamation, [91] but also in litigation for other negligent postings of material deemed harmful or injurious. [92] In fact, one could argue that the protection afforded by 47 U.S.C. §230 offers greater protection against online service providers than would most defamation statutes against a publisher in the print world. Section 230 is becoming a mega-immunity statute, protecting online service providers from many types of civil harms. [93] A practical result is that individual actors who are harmed may find their remedies limited, as the intermediary actor is now insulated from liability, while pursuing remedy against the individual defamer is impractical. [94] This raises the question of where it is most logical to place the responsibility for enforcement and remedy: at the online service provider/intermediary level or with individual actors (*i.e.*, aggrieved parties needing to sue the offending party)?

{38} This expansion of control and regulation through law is indicative of redactive information environments. One practical result is that, because plaintiffs can no longer sue service providers, as those providers now have immunity under the law, the only recourse is to suffer the harm or to proceed after individual litigants. The latter option is sometimes not viable because it is either cost-prohibitive, the individual publishers-posters are judgment proof, or online service providers are reluctant to release the name of an individual poster from their internal records. As a result, the law, while curtailing litigation against service providers, may make the actual perpetrators of the harm less likely to be held responsible because of the difficulty of individual litigants pursuing remedy and receiving compensation for harms. This result is far less efficient than the recent law, also part of the Digital Millennium Copyright Act, [95] discussed earlier, that arbitrates similar disputes against online service providers for postings of infringing copyright materials by third parties on their systems. [96] The new law assigns liability to the service providers only if it had knowledge of the infringing posting and failed to take appropriate action to remove it.

C. *Emergence of Self Protection Measures Increase: Information Reaction*

{39} The information environment of the post-national era is characterized by flux. The two trends discussed thus far, iteration, which is the inadequate application of legal norms to cyberspace in arbitrating information disputes, and redaction, which is the expansion of legal norms to cyberspace in an attempt to regulate information, pave the way for yet a third trend. As a result of the uncertainty in the ability of the law to preserve the information status quo, policymakers, with the support of information owners, have reacted by seeking alternative measures to protect their interests. Two examples are the *sui generis* database protection legislation discussed earlier and another *sui generis* protection measure passed to protect high technology mask works and products in semiconductor computer chips. [97] The latter *sui generis* legislation blends copyright, patent trademark, and patent regimes into a "super hybrid high law" that protects United States high technology through the exclusive grant of chip production rights for up to ten years.

{40} A similar market-oriented protectionism response was recently instituted in the area of trademark infringement that established controls against the importation of "gray market" goods into the United States. Self-protection information environments typically develop in response to control gaps left by the failure of iteration or redaction. Self-protection measures can be instigated by individual information owners to protect their interests or by policymakers concerned about maintaining the strength of national interests. It can also be viewed as a response to the jockeying by commercial entities for market advantage that ensues as a result of the harmonization and globalization processes.

{41} As an example, "gray market" protection in the United States has increased in response to a recent

decision by the Supreme Court in *Quality King Distribs., Inc. v. L'anza Research Int'l, Inc.* [98] Two intellectual property scholars surmised that, "[t]he gray market is a multibillion-dollar industry based on the importation of copyrighted or trademarked materials without consent of the owner of those intellectual property rights. This parallel importation creates a second, unauthorized distribution system that competes with the domestic system authorized by the manufacturer." [99] The Supreme Court decision has controlling significance for "gray market" importation in the entertainment, publishing, and other copyright industries. [100]

{42} In its opinion, the Supreme Court indicated that the importation right under 17 U.S.C. § 602 is part of the distribution right under 17 U.S.C. §106. This distribution right is, in turn, limited by various provisions of the copyright law, such as the fair use provision of 17 U.S.C. §107, and the first sale doctrine, as expressed in 17 U.S.C. §109. The first sale doctrine is a statutory expression of the perpetuity concept; it limits the copyright owner's right to control the subsequent disposition or transfer of legitimate copies of the work after the first sale is made. According to the Court, the copyright law would not operate to protect the domestic sales due to the first sale doctrine. The first sale doctrine, like the concept of fair use is an access right that insures that public good is served by excepting from the copyright owner's exclusive rights, uses or transfers of the work by others.

{43} Commercial entities were left seeking other protection measures in the wake of the Supreme Court *Quality King* decision. In essence, the Court recognized a "loophole" for gray market goods. This occurs when a United States domestic company sells or exports the product to a foreign entity, often at a lower price that is consistent with the anticipated revenue of the foreign market. It is obvious that the domestic company-exporter cannot control the resale of the product by the foreign entity at this point in the scenario. The foreign entity then imports the product back into the United States and the product is sold below the domestically-priced product by a third party. This interferes with the domestic sales of the product by the domestic company. It is at this point that domestic companies attempted to control the resale of the product in the United States, but were thwarted by the Supreme Court's application of the first sale doctrine. Now, the International Trade Commission, upon a filing of a complaint by an aggrieved party whose products are re-introduced into United States markets, will issue an exclusion order, as well as a civil penalty up to $100,000 per violation that prevents importation of the "gray market" product into the United States. In the past, the exporter would have had to file time-consuming and expensive suits against individual importers. [101] In a similar fashion, this preventive mechanism is analogous to the European Commission's decision to ban the existence of duty-free shopping in member states by June 30, 1999.

{44} The import controls placed upon the competition to a nation's intellectual property markets is an example of self-protection measures enacted to respond to a threat, perceived or real, that policymakers view as a challenge to their control over the information. In other cases, the individual commercial entities within the sovereign state or multi-state may, with national endorsement, construct their own protective reaction measures. An example of this is the recent development of copyright management systems. The major Clinton Administration blueprint for copyright reform, the "White Paper" [102] advocates the use of encryption, digital signatures, and stenography that consists of watermarking or codes, which would be embedded in copyrighted works and would function as identification, tracking, and use signatures.

{45} This electronic "lock and key" solution to copyright infringement in digital settings was accepted as part of the settlement in *Frank Music Corp. v. CompuServe, Inc.* [103] In addition to $568,000 in damages, CompuServe agreed to administer the online licensing scheme. In the *Frank* case, music publishers alleged that a CompuServe bulletin board system ("BBS") connected to the Internet allowed users to download copyrighted songs. According to Raysman and Brown, [104] the settlement-licensing scheme could develop into an industry standard. If these digital gate-keeping technologies are adopted, one result might be that every use of copyrighted material would entail a cost to the user, in spite of fair use concepts. This would represent a drastic change in the extent of the public information space available. [105] Further, Congress has

provided its tacit endorsement of these measures by passing legislation prohibiting the removal or alteration of such copyright management information if the intent is to induce infringement. [106] The selling of copyright management circumvention devices is also prohibited. The law also implements the recent WIPO copyright agreements discussed earlier in this article.

D. *The Loss of Public Space: Information Marginalization*

{46} There is a loss of public space when information becomes marginalized. This occurs as commercial interests supercede cultural or educational information interests. The problems that result when harmonization or globalization mechanisms fail to incorporate or to accommodate indigenous or cultural attitudes towards information have been presented earlier. Two other examples serve to demonstrate this principle. Recent discussions focusing on the expansion of top-level domain name suffixes have focused predominantly upon commercial interests. New names will include the following: ".firm" for businesses or firms, ".store" for businesses offering goods for purchase, ".info" for businesses providing information services, ".web" for businesses providing web services, ".arts" for cultural and entertainment activities, ".rec" for businesses involved in recreational activities, and ".nom" for domain names for individuals. [107] Absent in the top-level domain name expansion are categories designed to guarantee the identification of sites designated for public inquiry, much like the public television, public radio, or local access cable lines that are currently reserved for public purposes. In addition, the use of ".XXX" for adult sites [108] or ".child" for those sites safe for children might also facilitate the Internet zoning approach Justice O'Connor advocated in her concurrence in the *Reno* decision. [109] A domain name, such as ".pub" might be used to distinguish those true public-oriented sites from general non-profit ".org" entities that are still "positional" in nature (*i.e.*, that in some way advocate or represent a particular position). Like the development of the Internet, but to a lesser extent, the development of the domain name registration system has been criticized for its emphasis on commercial and other private interests to the exclusion of public interests. [110] The dominance of virtual location devices, or domain names geared towards commercial or private interests is another indication that commercial or other private interests are permeating the World Wide Web.

{47} The digital environment was also seen as an opportunity for the privacy interests of children to be marginalized. In the early 1990's, the practices of online marketers in targeting children as research targets came under scrutiny. [111] Children were often unknowingly, due to sub-developed consumer acumen, releasing vast amounts of personal information about themselves and their families. The lack of consumer savvy in children, coupled with the ease of engaging children online and soliciting information from them in network environments, allowed marketers to circumvent the normal protection parental supervision offers. While there is a rich depository of literature supporting the protection of children in a broader human rights capacity (*e.g.*, health, education, and other general welfare issues), [112] little thought was given to the protection of children in a market or consumer context. The network environment challenges existing thought concerning the topics within which child welfare issues are debated. [113] For example, inquiry was often disguised in the form of a game, contest, or club. Further parental authorization was not sought. Existing law provided limited application. The collection and use of consumer information under circumstances that are false or misleading is an unfair trade practice. [114] However, specific statutory protections, as opposed to reliance on federal regulatory oversight alone, were sought. [115] As a result, the COPA [116] was passed in essence, to codify the Federal Trade Commission's position.

{48} Another example of the marginalization of World Wide Web users is occurring in American distance education environments. Web-based distance education students have fewer fair use rights than their "live" counterparts at the same university. The problem arises because it is unclear, the extent to which, the concepts of fair use contained in 17 U.S.C. §107 and the educational "fair use" guidelines drafted under that section, [117] apply to distance education settings. More importantly, other sections of the copyright law designed to allow educational uses of copyrighted material in the classroom may not translate well to the distance

education environment. For example, 17 U.S.C. §110, does not, as written, allow for such performances or displays over the Internet. Section 110 allows educators to show, perform, or display copyrighted works, such as video cassette recordings to a live classroom, as long as the subject of the video is related to the course content and the showing is to class members only. There is no provision to allow for the showing of the same video to students in a web-based course, not to that portion of students in a class who are web-based. In fact, under a reasonable reading of the current law, that act is prohibited. These web-based, virtual students are penalized simply because of the nature of their spatial interaction with the classroom teaching environment, *i.e.*, because the students are in a virtual classroom. [118] In this way, the information interests of web-based students under current copyright law are marginalized.

III. Applications: Internet Myths And Realities

{49} This article concludes with a review of several myths that are often forwarded in the debate against those who attempt to regulate, through law, conduct in cyberspace. The myths are not so much rebutted with alternative maxims, but questioned in the hopes of forwarding an understanding of why these legal controversies have developed - and will continue to develop - in cyber society. The first myth is a general statement that conduct and content cannot be regulated on the Internet through law because the Internet is an open system, with no boundaries, and thus, law cannot practically apply. Another myth is that the best characterization of the Internet is that of "last frontier." In this characterization, virtual space may or may not be limitless, but there is much uncharted territory, and those who stake their claim to it first will come to control it. It forwards a first come-first serve, "most powerful-most control" attitude towards cyberspace. Next, the concept of the Internet as virtual "green space" or a commons is critiqued. In this modality, the public nature of the Internet must be preserved at all costs. Unfortunately, like the green spaces of old, degradation of this commons can also occur in the context of cyberspace. In contrast, the reality of recent World Wide Web litigation suggests that society is already adopting legal concepts and nomenclature to concepts of virtual spaces, *i.e.*, with the emergence of terms like "cybertort" and "cyber squatter." All of the myths in some sense presuppose an attitude of less law or a lesser role for public governance than currently exists in physical space. It is as if proponents of these models view the Internet as their last chance for anarchy, or at least for regulatory climates on terms which envision the proponents of a particular myth to be in control of the information access and use rights of others.

A. *The Myth of Virtuality*

{50} The first myth is a general statement that conduct and content cannot be regulated on the Internet through law because the Internet is an open system, with no boundaries, and thus, laws cannot practically apply. This myth is rooted in the belief that the Internet is so new that present social norms and institutions are unprepared to fathom its workings and to interact with technology in a reasonable, socially structured way. For example, proponents such as Peter Huber would remove any role for public governance vis-à-vis the legal regulation of communicative behavior. [119] Proponents of this view have called for the cessation of intellectual property right principles in cyberspace as well, and they advocate a move towards private laws or completely self-regulating norms. [120] This view is the perspective of "Internet libertarianism" taken to its logical and extreme conclusion. This idea itself is based upon the inability of the medium or technology to control information flows. For example, a statute of one country forbidding the sending of obscene information cannot practically control senders of the material in another country. [121] At best, such laws can be designed only to control the receipt of information. In theory, this over-taxes the information system as undesirable information makes its way into the system, or onto the Internet in this case, before it can be regulated. Control exists only at the down-stream end. Similarly, recent developments in copyright management technology work the same way. [122] The technology does not necessarily work to prevent illegal uploading of pirated material onto the Internet, but renders its down-stream use, such as the downloading of a copy, unusable or traceable.

{51} It is not clear what type of order, if any, would exist in this "Internet of virtuality." However, it seems an unsound course upon which to embark. This is so for several reasons. First, the law is already adapting existing principles to various Internet controversies. True, courts and legislatures still struggle against each other over which particular path to take. For instance, the battle over content regulation on the Internet recounted in the *Reno* decisions [123] provides a case in point. Yet, the paradigm of Internet law that is developing is, for better or for worse, based upon existing legal maxims. There will always be adjustment in law, but the law's ability to adapt, to remain in flux and uncertain at times, is also its blessing in the post-national era. The law currently allows order in cyberspace to develop within the existing legal information infrastructure. Terms such as "cyber squatter," "cybertort" and "cyber smear" [124] indicate that the application of known legal tenets to the Internet is possible and even desirable. If this ordering does not occur, what is left? Would self-regulating mechanisms develop equitably on the Internet without public governance or intervention?

{52} Perhaps less overt, but nonetheless pernicious is the increase in the number of advocates for self-normative regulation of the Internet. In reality, this option envisions a series of private rights as the dominant mode of information access vis-à-vis the freedom to contract. Without a system of public law, private interests will dominate the rights of parties in information transactions. In this case, contract will dominate relationships between remote Internet actors. This is unsound for two reasons. First, it assumes some normative structure to enforce the contract or game rules in the first instance. Thus, the proponents of Internet virtuality see the role of public law as rather self-serving of private interests, *i.e.*, contract enforcing or at least contract regulating. Second and most important, it requires parity among actors, which is simply not the case on the Internet. This is problematic because equitable contract rights are premised upon the somewhat equal and consistent bargaining right of the parties. In contract law, an agreement drafted unilaterally by a dominant party and then presented on a "take it or leave it basis" to the weaker party with no real opportunity to bargain concerning the terms of the agreement is known as a contract of adhesion. [125] Adhesion contracts may be voided on the grounds that this uneven distribution of bargaining power, if exercised, would result in a contract that is unconscionable, and thereby against public policy. The shrink wrap license illustration discussed earlier in this article is often cited as an example of an adhesion contract. [126] If the so-called "information poor" are left to their own devices with the unequal bargaining that results from this position, to acquire the means for improvement, there is little hope for true information equity. A new term, "information adhesion" is used to describe the process of market-based information alignment and control, that, in the present discussion is expressed through the mechanism of private contracting, favors those with a dominant bargaining position, and results in information inequity. This "adhesion of information" can occur where the parties are nation-states or within a state between commercial owners and individual users of information, as the *ProCD* litigation and U.C.C. and UCEDA reforms suggest.

{53} Third, assuming that natural progression self-regulating or private contracting schemes result in survival or dominance of the economically or politically fittest, those who are at an advantage will remain so. Moreover, without a system of public laws that reserve and protect the public interest, new communication technologies will become vehicles for further subjugation of lesser actors instead of liberating media. The problem with this approach is that, while it may offer opportunities and incentives for new economic and other development free from state regulation, it also assumes a certain parity among remaining actors, or put another way, it places a moral imperative on subsequent transactions. It may not matter to individual users of the Web who desire to order concert tickets if Microsoft in-links to the Ticketmaster site. [127] It may at first appear that many disputes do not affect individual users. Consider disputes that occur between unequal commercial actors in vertical competition markets: from service provider to bulletin board operator and then downward establishing individual liability for copyright infringement or tortious act, *e.g.*, the *Netcom* and *Zeran* situations. Likewise dominant information stakeholders may also compete in similar horizontal markets, as was depicted by the NBA game pager litigation involving competition among providers of real time game scores. [128]

{54} However, the precedent established in these controversies will control when individuals interact through the contract model with these larger private or commercial actors. The *ProCD* litigation and developments in U.C.C. Article 2b revisions suggest a growing acceptance of this model that is disturbing. Many participants similarly situated to Zeidenberg will not have the bargaining power to negotiate, and so must take what information owners offer on owners' terms or take nothing at all. This scenario creates a parity dynamic. Private law need not replace public law in Internet settings; in fact, the latter may bring stability to the Internet. Furthermore, there is evidence to suggest that traditional legal precedent is overriding what Internet customs or self-governing practices have arisen. [129]

B. *The Myth of the Last Frontier:*

{55} Related to the virtuality myth is a position that attempts, at least in the United States, to hearken back to bygone days of the westward expansion of the American Frontier. In a global context, this might be akin to the days of world discovery and colonization. This myth presumes a certain manifest destiny to the Internet as well. [130] The myth is based upon the "cult of bigness" and limitless space that dominates the expansionist and territorial designs of the elite. [131] The view might best be articulated as the myth of the Internet as the "last frontier." But, this myth is problematic for several reasons. While some attributes of the Internet might fit within this rather romantic notion of technology, it too suffers from a belief that an unregulated climate is the best one in which to base Internet participation. This perception is related to the myth of viruality, but whereas, virtuality anticipates self-regulating normative structures to dominate information transactions, the myth of the Internet as a "last frontier" sees no role for normative behavior whatsoever. Often, this movement is associated with the original hacking and cyber-counter-culture that developed in the early days of the Internet. [132]

{56} Like the frontier land and resource-consuming perspectives of the early settlers, the "cult of bigness" sees ownership and property accumulation as a "good" in and of itself. Instead of pitting the fences of the sheep ranchers and the homesteader against the open range of the cattle drovers, the myth of the Internet as one of the "last frontier" places, contrasts for example, the commercial interests of the website owners against free-link proponents. Social mobility is symbolized in the ability to own or control property, real or virtual. Those who do not own property in their own right are trespassers. Applied to the Internet, it relegates those without the information, poor or needy, as mere interlopers, but never true participants.

{57} Underlying this myth is the belief that in a completely open and unregulated frontier system, limitless opportunity will abound. [133] Yet, this is simply not the case with the Internet. Some mechanisms actually work less well in cyberspace. Consider the problem of domain name registrations discussed previously in this article. Instead of a "last frontier" for trademarks in cyberspace, the limitations of technology actually make the development and use of trademarks as domain names in cyberspace less available. There are other legal anomalies in the transition from physical to virtual reality of the cyberspace last frontier. If the Internet, as the "last frontier" analogy, is to have merit, then the ability to move into new virtual frontier property spaces, should expand, not retract. This is not occurring; rather, quite the opposite transpires. It is in the application of a traditional property right, *i.e.*, trespass, [134] that ownership rights in cyberspace have actually expanded, resulting in a decrease in the ability to move within cyber-information-space. This can be evidenced in the expansion of personal property rights in individual cyberspaces such as e-mail accounts. This "fencing-in" phenomenon would be in direct opposition to the limitless space of the manifest destiny of the "cyber-frontier" model. To some extent in web-link controversies, [135] but more interestingly, in e-mail communications, the assent of privacy concepts to protect recipients from unwanted solicitations emerges to the forefront. This privacy right, based upon the property law doctrine of trespass as applied to the virtual space, has been held to protect personal e-mail space. [136] This propertization of cyberspace is antithetical to the notion of it as being a "last frontier." Strangely, this application of trespass to cyberspace creates far greater privacy rights for consumers in the cyber-marketplace, than currently exist in the physical space of

traditional mail or analog communications. The use of criminal sanctions in the junk e-mail privacy cases [137] is also increasing the height of the cyberspace fences that can be constructed.

{58} Finally, reliance on the "last frontier" model of cyberspace leads to an environment in which any arbitration is metered out, like in the days of the Old West by vigilante justice. Those with the fastest gun were usually correct, as those who opposed them were not around to ask questions. Likewise, the development of information vigilantism resulted in an Internet environment where private interests will operate completely unregulated, either against public interests or other less substantial private interests. Without any public governance, the only legitimizing act of information use is found in its access or the control over its access. If one obtains access to the information or control over others' access by whatever means available (*i.e.*, through the process of information vigilantism), it will be deemed a legitimate access, in so far as the information vigilante is concerned. Without public governance over the information, those without the information must also resort to vigilantism to obtain access to the information, as the process is further rationalized. Gone are the concepts and mechanisms that attempt to identify proper from improper acquisitions, such as trade secret and misappropriation of business information, or copyright and fair use of published material. Furthermore, the only recourse is also vigilantism. In the online environment, this means that a remedy is chosen from one of three possible courses of action. First, one can re-acquire or steal the information back. Second, one can acquire or steal other information in its place, possibly, in a spirit of retaliation. Third, one can engage in self-protection measures, which may or may not be possible or affordable by the information victims. Faced with these limited alternatives, this model may even stifle competition because legitimate business enterprises will be reluctant or unable to venture into this environment. The only rule of law is whether the information can actually be accessed or downloaded, scanned, etc., but not whether it is proper to do so. Thus, to the information vigilante, access or acquisition is synonymous with the right to the information.

C. *The Myth of "Internet Commons" or "Green Space"*

{59} A final myth that tends to support a desire for less traditional legal structure in cyberspace is a view of the Internet as a gigantic "commons" or "green space." This myth envisions slightly more order than the "last frontier" ideology, but still believes that unlimited public spaces are possible in cyberspace. It is a desire for lawlessness as well, but instead of coming from a commercial or private enterprise, like the virtuality myth, or the reactionary elements of the cyber- counter-culture or vigilantes under the "last frontier" myth, it comes instead from the public interest proponents. [138] In principle, there is nothing unsavory in this view. However, like the other two model-myths, it also does not adequately characterize the reality of the Internet, and like the other two myths, if embraced, will do more harm than good. Perhaps one flaw is that it ignores the contribution that the private sector and rules of law are making towards universal access on the Internet. Like it or not, it is the private sector, in the United States, that is bearing the financial burden for the construction of the technical information infrastructure. It does not seem unreasonable that the legal information infrastructure should reward, within limits, these efforts. Still, a closer look at the myth of the Internet as a "commons" or "green space" is warranted.

{60} Like the "commons" or "green space" concepts of old, the tragedy of the commons is that, if use of the commons or common space is left completely unregulated, the space will be overused and eventually no one will be able to benefit from it. [139] The question is whether this analogy holds true for the Internet, both in terms of its use and abuse. In terms of use, the Internet is certainly like a "commons" where people can gather, find common interests and communicate. In fact the analogy of the "green space" has been applied to new communication technologies such as cable. [140] Other commentators have discussed whether certain elements of cyberspace are akin to a public forum under a traditional free speech analysis. [141] The concept of a public forum in First Amendment jurisprudence is based upon the concept of protected speech, such as those words spoken on the town "green space" of the Early-American colonial village.

{61} Yet, in terms of abuse, the space of the World Wide Web, for example, would certainly appear limitless and guarded only by the confines of developing technology. For instance, there seems to be the potential for millions of additional sites on the World Wide Web, which would represent millions of additional publishers and users. On the other hand, commentators, such as Gladstone, [142] argue that viewing the Web as another common marketspace, a "sprawling mall offering goods or services" or perhaps a "vast library," for example, [143] is unsound. However, the argument could be made that the "commons" is nonetheless being degraded. This might hold true for two reasons. The first consideration is degradation in terms of content and context. While questionable speech, such as that which is harmful, like hate sites or bomb-making pages, obscene, indecent, or otherwise offensive has a place on the Internet, it might still represent some lesser-valued information for most users. [144]

{62} In American jurisprudence, the Supreme Court has recognized that certain types of speech fall outside of the protection of the First Amendment. [145] Implicit in this hierarchy of speech is an underlying assessment that identifies some speech as less worthy of protection than other types. In *Roth v. United States*, [146] the Supreme Court observed that, "implicit in the history of the First Amendment is the rejection of obscenity as utterly without redeeming social importance." [147] While this content has a right to exist, should it dominate the make-up of the World Wide Web? [148] Likewise, could one ask whether the Internet's value, in terms of context, as a medium of information transfer or an information resource is being degraded due to the proliferation of personal sites on the Web?

{63} Additionally, in the print or analog marketplace, traditional editing mechanisms do operate as filters of sorts on less desirable content, by naturally screening out material that editors and publishers believe will be of little interest, in terms of potential marketability, to the public. The result is that the information dissemination publishing system limits the amount of information available at any one time. [149] This availability issue raises the concept of information overload or noise in the context of the Internet. [150]

{64} While it might empower a personal website owner to be able to create their own site, does it really matter to individual X that individual Y who is on the other side of the country enjoys taking pictures of the moon or is placing live images of their cat online? Does this add to the quality of life, does it detract from the usefulness of the Internet as an information system? This line of reasoning recalls another theory in information science which maintains that in any information system, a sizeable portion of the information will be of lesser or mediocre quality. [151]

{65} As more and more information is available on the World Wide Web, locating and using information in an effective manner becomes more and more difficult. This information overload might be likened to a degradation of the "information commons" to the extent that a "commons" does exist in cyberspace.

{66} Finally, a complete reliance on this principle ignores the role of private spaces as well. When private rights are awarded and the use of some property is limited or subject to ownership rights, there is also a preservation of that space, in terms of overuse or in terms of the abuse of the rights of the space-holder. It is true that in a technological sense, space is unlimited on the Internet and anyone can be a publisher. In the analogy presented, an argument might be made that the world would never run out of the "Internet Commons;" yet, there is a slow pollution of the quality of the information space from overload and from offensive, dangerous, and erroneous content. Property rights can therefore serve a purpose, [152] as they prevent the overuse of the "information commons," curtail information overload, and like the zoning laws of modern real property law, carve out spaces for particular uses.

IV. Conclusion And Future Perspectives

{67} What are the challenges facing the legal infrastructure in the post-national era? The first challenge is to reject harmonization when that process results in the domination of external forces upon the governance of an

individual state or multi-state entity. Likewise, should caution be extended to various globalization efforts that attempt to place commercial interests above other interests of a state or its citizenry? In contrast, efforts to incorporate or preserve the cultural or information integrity of the citizenry should be attempted.

{68} Sovereign states or multi-state entities will continue to respond through law to the challenges of the digital environment. While the application of law to cyberspace is under development, there is the potential that a loss of information access and equity will occur. This loss may result as when traditional information boundaries breakdown (*i.e.*, iteration) and new meta-information boundaries arise (*i.e.*, redaction). There is no longer a check vis-à-vis the legal infrastructure on the private stakeholders whose interests may be in opposition to the public good. Furthermore, sovereign states or multi-state entities should resist the tendency to adopt self-protection measures under a reaction approach that may restrict the flow and access of information, and should also be weary of the marginalization of the public interest or of particular stakeholders whose interests may not otherwise be protected.

{69} Finally, designers of the legal information infrastructure in the post-national era must be aware of certain myths that may permeate the attitudes of various global information infrastructure ("GII") stakeholders. The Internet may, at times, resemble a model that is unlike any other community (*i.e.*, virtuality). The Internet may also exhibit the character of a "last frontier" or be akin to a "public commons" or "green space." But, no one model, though contributing to an understanding of the Internet, can serve to explain all of its nuances in all settings. Planning the future of the GII with an awareness of these concepts and the potential negative effects that unreasonable reliance on any model one could produce will result in the design of optimal social, political, economic, and legal infrastructures that are most beneficial to world citizenry.

ENDNOTES[**]

[*] Mr. Lipinski is an Assistant Professor and Co-Director, of the Center for Information Policy Research at the School of Library and Information Science, at the University of Wisconsin in Milwaukee. He earned his J.D. from Marquette University Law School in 1984, and his LL.M. in 1986 from The John Marshall Law School. Mr. Lipinski earned his Ph.D. in Information Science in 1998 from the University of Illinois at Urbana-Champaign. Mr. Lipinski has worked in a variety of legal settings, including the private, public, and non-profit sectors.

[**].**NOTE:** All endnote citations in this article follow the conventions appropriate to the edition of THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION that was in effect at the time of publication. When citing to this article, please use the format required by the Seventeenth Edition of THE BLUEBOOK, provided below for your convenience.

Tomas A. Lipinski, *The Developing Legal Infrastructure and the Globalization of Information: Constructing a Framework for Critical Choices in the New Millenium Internet -- Character, Content and Confusion*, 6 RICH. J.L. & TECH 19 (Winter 1999-2000), *at* http://www.richmond.edu/jolt/v6i4/article2.html.

[1]. This article is based on a paper entitled *Globalization of Information and the Post-National Era: Critical*

Choices for the New Millennium and Beyond, presented at The Moral and Legal Challenges of the Information Era Conference, University of Pretoria, Pretoria, South Africa, May 24 & 25, 1999 (manuscript on file with the author).

[2]. *See* Treaty of Certain Questions Concerning the Protection of Literary and Artistic Rights (1996), retitled the WIPO Copyright Treaty; and Treaty for the Protection of Rights of Performers and Producers of Phonograms (1996), renamed the WIPO Performances and Phonograms Treaty, adopted December 20, 1996; *see also* WIPO, *Texts of Treaties Administered by WIPO* (visited Dec. 31, 1999) <http://www.wipo.org/eng/iplex/index.htm>.The Treaty on Intell. Prop. in Respect to Databases (1996) is still under negotiation; Colm P. MacKernan, *WIPO Treaties Will Create Significant New Rights For Copyright Holders* (last modified Apr. 7, 1997) <http://www.ablondifoster.com/library/wipo.htm>(stating "[t]he first two of these treaty drafts were finalized and adopted [on December 20, 1996] . . . the last treaty relating to databases was not accepted and will be the subject of further negotiation").

[3]. Pub. L. No. 105-304, 112 Stat. 2860 (1998).

[4]. *See generally* Robert M. Sherwood, *Why a Uniform Intellectual Property System Makes Sense for the World*, *in* NAT'L RES. COUNCIL, GLOBAL DIMENSION OF INTELL. PROP. RIGHTS IN SCI. AND TECH. 68, 68-70 (1992) (discussing four requirements or characteristics: non-identical provisions, congruence, stimulation and comprehensiveness). Mr. Sherwood notes that "harmonization of laws, procedures, and rules for every country is not called for, although that could follow. . . ." *Id*. at 69.

[5]. Council Directive 96/9/EC, preamble, 1996 O.J. (L77) 20.

[6]. *See id*. at para. 1-3 (noting the need for the directive due to the following rationales: a lack of adequate protection of databases among all Member States, a lack of harmonization of laws, and the negative effect on internal markets resulting from differing legal protections).

[7]. *See* Collections of Info. Antipiracy Act, H. R. 2652, 105th Congress (1997); Collections of Info. Antipiracy Act, H.R. 352, 106th Congress (1999).

[8]. *See* U.S. COPYRIGHT OFFICE, REPORT ON LEGAL PROTECTION FOR DATABASES 45 (1997); Tomas A. Lipinski & Steven Heser, *The Commodification of Infrastructure Information in Proprietary Databases: A Policy Assessment* (article in progress and unpublished manuscript on file with author).

[9]. *See* Feist Publications v. Rural Tel. Serv. Co. Inc., 499 U.S. 340, 359-61 (1991) (rejecting the "sweat of the brow" doctrine).

[10]. *See* Andrew L. Deutsch, *Congress to Consider Data Base Bill*, NAT'L L. J., Oct. 20, 1997, at C3 (discussing a possible concept of database protection that Congress may consider that was offered in the *Report on Legal Protection For Databases* issued by the Copyright Office).

[11]. *See* Julius J. Marke, *Database Protection Bills Pending in Congress*, N.Y. L. J., Aug. 17, 1999, at 5 (discussing the library community's opposition to The Collections of Info. Anti-Piracy Act, H.R. 354, 106th Congress (1999)).

[12]. *See* Claudio R. Frischtak, *Harmonization Versus Differentiation in Intellectual Property Right Regimes*, *in* NAT'L RES. COUNCIL, GLOBAL DIMENSION OF INTELL. PROP. RIGHTS IN SCI. AND TECH. 89, 99 (1992) stating,

> [t]he fundamental trade-off that policymakers face in the choice of an optimal IPR [Intellectual Property Rights] regime in the current international environment is simple to state: closed-

economy considerations of potential gains from and IPR regime tailored to the country's circumstances may have to be balanced against open-economy income losses from reduced levels of trade and investment, if the choice of IPR regime is inconsistent with the trading/investment partners' interest.

Id.

[13]. *See, e.g.*, Raymond T. Nimmer, INFO. LAW ¶ 1.02 and ¶ 1.04 (1999) (noting the shift in economic values from the tangible to the intangible (information) and how "[t]rade in information in developed countries far exceeds the importance of trade in goods."). *Id*. at ¶ 1.04; NAT'l TECHNICAL INFO. SERV., U.S. DEP'T OF COMMERCE, THE EMERGING DIGITAL ECONOMY II (1999) *available at The Emerging Digital Economy II* (visited Feb. 1, 2000) <http://www.ecommerce.gov/ede/report.html>.

[14]. *See* Tomas A. Lipinski, *Information Ownership and Control*, *in* 33 ANNUAL REV. OF INFO. SCI. AND TECH. 1- 38 (1999) (reviewing recent trend relating to digital information in which information ownership is encroaching on public use of information).

[15]. *See generally* Raymond T. Nimmer, THE LAW OF COMPUTER TECHNOLOGY: RIGHTS, LICENCES, LIABILITIES ¶ 5.02, at 5-3 to 5-8 (1992) (discussing technology licensing contracts in a "new, mass-market environment"). *Id*. at 5-3; Joseph Migga Kizza, CIVILIZING THE INTERNET: GLOBAL CONCERNS AND EFFORTS TOWARD REGULATION 28-29 (1998) (noting the impact of the Internet on creating a global marketplace).

[16]. *See generally* Cees J. Hamelink, CULTURAL AUTONOMY IN GLOBAL COMMUNICATIONS: PLANNING NAT'l INFO. POLICY 110 (1983) (considering the fiscal decisions regarding national control of information systems); COMMUNICATION AND DEMOCRACY 203 (Slavko Splichal & Janet Wasko, eds., 1993) (noting international companies offer interactive media to the public but the systems are "not designed with democracy in mind;" they are designed to be very profitable).

[17]. *See* Edwin Mansfield, *Unauthorized Use of Intellectual Property: Effects on Investment, Technology Transfer, and Innovation*, *in* NAT'L RES. COUNCIL, GLOBAL DIMENSION OF INTELL. PROP. RIGHTS IN SCI. AND TECH. 107 (1992) (discussing effect of weak intellectual property protection on developing countries).

[18]. Friedl Weiss & Paul De Waart, *International Economic Law with a Human Face: An Introductory View*, *in* INTERNATIONAL ECONOMIC LAW WITH A HUMAN FACE, 1, 4 (Friedl Weiss, et al. eds., 1998).

[19]. *See* Angela J. Campbell, *Universal Service Provisions: The "Ugly Duckling" of the 1996 Act*, 29 CONN. L. REV. 187, 187 (1996) (noting the disparity of access to communications technologies in America); Tomas A. Lipinski, *Legislating an Information Underclass and the Statutory Limits of Universal Service: A Critique of Section 254 of the Telecommunications Act of 1996* (1998) (unpublished manuscript, on file with the author).

[20]. *See* R. Michael Gadbaw & Leigh A. Kenny, *India*, *in* INTELLECTUAL PROPERTY RIGHTS: GLOBAL CONSENSUS, GLOBAL CONFLICT? 104, 104-05 (R. Michael Gadbaw & Timothy J. Richards eds. 1988) (discussing piracy in India and Hong Kong). *See generally* OFFICE OF TECH. ASSESSMENT, INTELLECTUAL PROPERTY RIGHTS IN AN AGE OF ELECTRONICS AND INFO. 211, 246 (1987) (discussing piracy of video and software by various countries).

[21]. *See, e.g.*, Philip W. Grubb, *Patents--Time for New Approach*, BUS. WIRE, July 17, 1999 (noting that India acceded to the Paris Convention and the Patent Co-operation Treaty); *India--IPRs--Some More Way to Go*, BUS. WIRE, July 5, 1999 (discussing India's patent protection); Kavitha Rao, *Sticking to Tradition*, ASIA WEEK, Aug. 21, 1998 (discussing the need to patent traditional Asian medical treatments to cash in on the

interest in alternative medicine in the West); Amy Louise Kazmin, *India to Sign Up to Patents Treaty*, FIN. TIMES (London), Aug. 14, 1998, at 4 (discussing India's recent accession to the patent co-operation treaty of the Paris convention); *Technology Innovation Key to China's Development*, XINHUA NEWS AGENCY, Aug. 22, 1999 (noting the need to protect intellectual property rights to foster new technology); *China Keen to Share Education Software Technology with Malaysia*, XINHUA NEWS AGENCY, July 10, 1999 (noting that China is interested in how Malaysia protects intellectual property) (all documents available in the LEXIS-NEXIS News Library).

[22]. Tomas A. Lipinski & Johannes J. Britz, *Deconstructing (the Concept of) Intellectual Property: Designing and Incorporating Alternative Models of Property Ownership in the New Millennium*, Paper presented at ETHICOMP 99, Fourth International Conference on the Social and Ethical Impacts of Information and Communication Technology, LUISS Guido Carli University, Rome, Italy, Oct. 6-7, 1999 (unpublished manuscript, on file with the author).

[23]. *See* Lawrence J. Goffney, Jr., *Digital Tech May Revolutionize Global Commerce: Technological Innovations May Facilitate a Shift Toward the Trade of Ideas Only Rather Than Goods*, NAT'L L. J., Oct. 23, 1995, at C23 (stating "[t]his last great revolution [the digital era] has created a new paradigm for world trade in which intellectual property is of paramount importance.") [hereinafter Goffney, *Jr., Digital Tech*]; Lesley Ellen Harris, DIGITAL PROPERTY: CURRENCY OF THE 21st CENTURY 35 (calling digital property the "currency of the twenty-first century") (McGraw-Hill Ryerson Ltd. 1997); Paul A. David, *The Global Dimension of Intellectual Property Rights in Science and Technology*, NAT'L RES. COUNCIL, GLOBAL DIMENSION OF INTELL. PROP. RIGHTS IN SCI. AND TECH. 3, 13 (1992) [hereinafter David, *The Global Dimension*].

[24]. *See* Doris Estelle Long, *The Impact of Foreign Investment on Indigenous Culture: An Intellectual Property Perspective*, 23 N.C. J. INT'L. L & COM. REG. 229, 243 (1998) (stating "[t]his transformation of 'indigenous culture' into a de-culturized, marketable commodity may be facilitated and, potentially even accelerated, by the development and enforcement of the intellectual property laws required to attract foreign investment."). *Id*.

[25]. *See* David, *The Global Dimension, supra* note 23, at 13; Claudio R. Frischtak, *Harmonization Versus Differentiation in Intellectual Property Right Regimes*, *in* NAT'L RES. COUNCIL, GLOBAL DIMENSION OF INTELL. PROP. RIGHTS IN SCI. AND TECH. 89, 94 (1992).

[26]. Goffney, Jr., *Digital Tech*, *supra* note 23, at C23.

[27]. *See* Ronald V. Bettig, COPYRIGHTING CULTURE: THE POLITICAL ECONOMY OF INTELLECTUAL PROPERTY (1996).

[28]. *See* Johannes J. Britz & Tomas A. Lipinski, *Deconstructing (the Concept of) Intellectual Property: Designing and Incorporating Alternative Models of Property Ownership in the New Millennium*, paper presented at ETHICOMP 99, LUISS Guido Carli University, Rome, Italy, October 6-8, 1999 (manuscript at 8-10, on file with the author), *supra* note 1;. *see also* an abstract of this paper *available at ETHICOMP99-Abstract* (visited Oct. 22, 1999) <http://www.ccsr.cms.dmu.ac.uk/conferences/ccsrconf/abstracts99/lipinskiII.html>.

[29]. *See generally* Peter Malanczuk, *Globalization And The Future Role Of Sovereign States*, *in* INTERNATIONAL ECONOMIC LAW WITH A HUMAN FACE, *supra* note 17, at 57 (discussing the multinational company's need to have international agreements to achieve predictability) (1998).

[30]. *See* Tomas A. Lipinski & Johannes J. Britz, *The Ownership of Intellectual Property in the 21st Century-*

-from Access to Control: Ethical Implications, paper presented at Computer Ethics: Philosophical Enquiry [sic] (CEPE'98), London School of Economics and Political Science, London, United Kingdom, (In Association with the ACM SIG on Computers and Society), Dec. 14-15, 1998 (unpublished manuscript, on file with the author).

[31]. Reno v. ACLU, 521 U.S. 844, 853 (1997).

[32]. *See* Mainstream Loudoun v. Board of Trustees, 2 F. Supp.2d 783, 793-94 (E.D. Va. 1998).

[33]. *Id*.

[34]. The Loudoun removal/selection distinction was based on the earlier Supreme Court discussion of the concepts in *Board of Educ., Island Trees Union Free School Dist. No. 26 v. Pico*, 457 U.S. 853 (1982) (finding a First Amendment limitation to the Board's ability to remove books from the school library). For criticism, see, for example, Donald J. Dunn, *Pico and Beyond: School Library Censorship Controversies*, 77 L. LIBRARY J. 435, 455 (1985) (stating "[c]ourts must understand that acquisition of an item for a library is different from weeding and removal. None of the three courts and ten opinions dealing with *Pico* seemed fully cognizant of these processes."). *Id*. (citation omitted).

[35]. Religious Tech. Ctr. v. Netcom Online Communications, 907 F. Supp. 1361, 1369 (N.D. Cal. 1995) (citation omitted).

[36]. *Id*. at 1378 n.25.

[37]. *See* P. Bernt Hugenholtz, *Adapting Copyright to the Information Superhighway*, *in* THE FUTURE OF COPYRIGHT IN A DIGITAL ENVIRONMENT 81, 92 (P. Bernt Hugenholtz ed., 1996) (stating "[i]n the 'paper' world, the act of reading a document or viewing a television program does not qualify as a restricted act. This may be different in the digital networked environment."); *see also id*. at 93 (noting "[t]he mere reception or consumption of information by the end user has traditionally remained outside the scope of the copyrighted monopoly. The transition into the digital networked environment does not, as such, seem to justify such a radical extension of the exclusive right.") *Id*. (citation omitted).

[38]. *See* Eric Fleischmann, *The Impact of Digital Technology on Copyright Law*, 23 NEW ENG. L. REV. 45, 46 (1988) (arguing that problems with copyright law due to advances in digital technology may undermine the intellectual property system); Mary L. Mills, *New Technology and the Limitations of Copyright Law: An Argument for Finding Alternatives to Copyright Legislation in an Era of Rapid Technological Change*, 65 CHI.-KENT L. REV. 307 (1989) (searching for an alternative to copyright law to govern new technology); and Pamela Samuelson, *Digital Media and the Changing Face of Intellectual Property Law*, 16 RUTGERS COMPUTER & TECH. L.J. 323, 340 (1990) (concluding that characteristics of digital media likely will "change the face of intellectual property law as we know it"); *see generally* Bernard Timberg, *New Forms of Media and the Challenge to Copyright Law*, *in* FAIR USE AND FREE INQUIRY: COPYRIGHT LAW AND THE NEW MEDIA 248, 262 (John Shelton Lawrence & Bernard Timberg eds., 1998) (stating intellectual property law will have to change to respond to technological advances).

[39]. *See* Yochai Benkler, RULES OF THE ROAD FOR THE INFORMATION SUPERHIGHWAY: ELECTRONIC COMMUNICATIONS AND THE LAW 663-80 (1996) (discussing the challenges posed by the digital environment for copyright law).

[40]. The characteristics of digital information is its malleability, mutability, transmissibility, and processibility, each raising or encouraging the potential for intellectual property owners; s*ee id*. at 21-34 (discussing the unique characteristics of electronic communications and digital information).

[41]. *See, e.g.*, Dennis A. Karjala, *Copyright and Misappropriation*, 17 U. DAYTON L. REV. 885 (1992) (creating a framework of copyright analysis in which misappropriation plays a role); Niva Elkin-Noren, *Copyright Policy and the Limits of Freedom of Contract*, 12 BERKELEY TECH. L.J. 93 (1997), *available at* (visited Nov. 19, 1999) <http://www.law.berkelye.edu:80/journals/btlj/articles/12-1/koren.html> (considering the unenforceability of contract rights due to a conflict with copyright law); James N. Talbot, *Facts, Copyright, Unfair Competition and Contracts*: *Will NBA v. Motorola Lead to Shrink Wrap Television?* 15 ENT. AND SPORTS LAW. 7 (1997) (searching for a legal theory to protect factual information); Charles R. McManis, *Do Not Support `Privatizing' Copyright*, NAT'L L. J., Oct. 13, 1997, at A24 (discussing efforts to create enforceable mass-market licenses).

[42]. *See* National Basketball Ass'n v. Motorola, Inc. and Sports Team Analysis, 105 F.3d 841 (2nd Cir. 1997) *rev'g*. 931 F. Supp. 1124 (S.D.N.Y. 1996), *amended* 939 F. Supp. 1071 (S.D.N.Y. 1996).

[43]. *See* The Washington Post Co. v. TotalNews, Inc., Case No. 97 Civ. 1190 (PKL) (S.D.N.Y. filed Feb. 20, 1997).

[44]. *See* David A. Rice, *Digital Information and Property and Product: U.C.C. Article 2b*, 22 U. DAYTON L. REV. 621, 643 (1997) (suggesting that a license is a disguised sale and that a "sale" should be a "license" subject to contract law). The text of UCITA can be found at *The National Conference of Commissioners on Uniform State Laws: Drafts of Uniform and Model Acts* (last modified Jan. 27, 2000) <http://www.law.upenn.edu/bll/ulc/ulc_frame>; *The Website Formerly Known as The 2BGuide* (last modified Dec. 14, 1999) <http://www.2Bguide.com>.

[45]. *See* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996), *rev'g* 908 F. Supp. 640 (W.D. Wisc. 1996) (holding that shrinkwrap licenses are enforceable as long as the licenses comply with general contract rules); *see also* Green Book Int'l v. InUnity Corp., 2 F. Supp.2d 112 (D. Mass. 1998) (considering terms of shrinkwrap license in determining merits infringement suit); M.A. Mortenson Co. v. Timberline Software Corp., 970 P.2d 803 (Wash. App. 1999) (finding the shrinkwrap license is enforceable).

[46]. *See* Feist Publications, Inc. v. Rural Telephone Serv. Co., 499 U.S. 340 (1991) (rejecting sweat of the brow doctrine and noting that facts are not copyrightable).

[47]. *See ProCD*, 908 F. Supp. at 646 (comparing the telephone listings copied from plaintiff's software and placed on the Internet to the uncopyrightable telephone listings in *Feist)*.

[48]. *ProCD*, 86 F.3d at 1453.

[49]. *See id*. at 1454-55.

[50]. *See id*.

[51]. Mark A. Lemley, *The Law and Economics of Internet Norms* (1998) (University of Texas School of Law) (unpublished manuscript, on file with author); Philip E. Agre, *The Market and the Net: Personal Boundaries and the Future of Market Institutions* (1998) (University of California, Los Angeles) (unpublished manuscript, on file with author).

[52]. *See* International Shoe Co. v. Washington, 326 U.S. 310, 317 (1945) (defining "presence" necessary to satisfy due process as "such contacts . . . with the state of the forum as make it reasonable . . . to require the corporation to defend the particular suit"). *Id*.

[53]. Julian S. Millstein, et al., DOING BUSINESS ON THE INTERNET: FORMS AND ANALYSIS, §11.02[2], at 11-13 (1999).

[54]. *See* David L. Mathus & Andrew M. Goldner, *Precautions Can Mitigate Legal Dangers of Web Sites*, NAT'L L. J., June 21, 1999, at C3 (summarizing recent cases determining jurisdictional issues involving websites); Mark A. Willard, *Two Concepts of Jurisdiction Cleave Courts*, NAT'L L. J., Aug. 30, 1999, at B7 (discussing recent cases that highlight differing concepts of jurisdiction offered by the courts); David S. Godkin & Marc E. Betinsky, *Personal Jurisdiction: If the [International] Shoe Fits, Wear It - But Does it Fit the Net?*, J. INTERNET L., July 1999, at 17 (discussing the applicability of traditional jurisdictional concepts with Internet use).

[55]. *See, e.g.*, Millennium Enterprises, Inc. v. Music LP, 33 F. Supp.2d 907 (D. Ore. 1999) (finding that existence of a website does not create general jurisdiction over the defendant and noting an absence of case law supporting such a proposition); Bensusan Restaurant Corp. v. King, 937 F. Supp. 295 (S.D.N.Y. 1996), *aff'd* 126 F. 3d 25 (2nd Cir. 1997) (holding that website without more, is insufficient to vest the court with personal jurisdiction over the defendant); Cybersell, Inc. v. Cybersell, Inc. 130 F. 3d 414 (9th Cir. 1997) (finding that webpage accessible to all users of the Internet is not a sufficient minimum contact for the court to exercise personal jurisdiction over the defendant).

[56]. No. 98-1749-A, 1999 U.S. Dist. LEXIS 8253 (E.D. Va. 1999).

[57]. Willard, *supra* note 54, at B14.

[58]. *See* Zippo Mfg. Co. v. Zippo DOT COM, Inc., 992 F. Supp. 44 (D.D.C. 1998) (employing use of a sliding scale of activity to determine personal jurisdiction); Mieczkowski v. Masco Corp. 997 F. Supp. 782 (D.C. Texas 1998) (finding 250 sales in the state of Texas and the potential for online contacts via e-mail justified the exercise of personal jurisdiction); SuperGuide, Corp. v. Kegan, 987 F. Supp. 481 (W.D.N.C. 1997) (advertising directed at residents of North Carolina but otherwise passive web presence sufficient); Inset Sys., Inc. v. Instruction Set, Inc. 937 F. Supp. 161 (D. Conn. 1996) (finding advertising via Web with a toll free number listed on site indicated intent to solicit business from citizens making long-arm jurisdiction proper); EDIAS Software Int'l v. Basis Int'l, 947 F. Supp. 413 (D. Ariz. 1996) (finding phone, fax, and e-mail communications sufficient to establish jurisdiction); Maritz, Inc. v. CyberGold, Inc., 947 F. Supp. 1338 (E.D. Mo. 1996) (finding collection of marketing information via website sufficient to vest personal jurisdiction where website contacted every user who accessed the site).

[59]. *See* Use of Electronic Media for Delivery Purposes, Exchange Act Release No. 33-7233 (Oct. 6, 1995).

[60]. Recounted in Godkin & Betinsky, *supra* note 23, at 19 (citing Stephan Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet?* (visited Nov. 15, 1999) <http://www.law.indiana.edu/fclj/pubs/v50/no1/wilske.html>.

[61]. *See* 15 U.S.C. § 1115 (b)(5) & (6) (1994 & Supp. 1997) (providing an infringement defense to those marks that were in use prior to the registration of the complainant's trademark but "only for the area in which the mark was used prior to such registration or such publication of the registrant's mark"). *Id*. § 1115 (b)(6).

[62]. *See* Dawn Donut Co. v. Hart's Food Stores, Inc., 267 F.2d 358 (2d Cir. 1959) (holding that plaintiff is not entitled to enjoin defendant use of trademark absent showing of a likelihood of consumer confusion about the source, sponsorship or affiliation of the product; *see also* Intermatic, Inc. v. Toeppen, 947 F. Supp. 1227, 1234 (1996) (stating that plaintiff must show likelihood of consumer confusion to establish infringement), *available at* <http://www.isc.meiji.ac.jp/~sumwel_h/doc/cases/Panavision_1998_USa9c.htm>.

[63]. *See Intermatic*, 947 F. Supp. at 1234 (noting that "unlike the typical trademark dispute, where both parties are using the name simultaneously and arguing whether confusion exists, the current configuration of the Internet allows only one party to the [disputed] domain name . . .[T]here does not currently appear to be a

way in which both [users of name] can both use the [domain] name"). *Id*.

[64]. *See* William A. Tanenbaum, *Intellectual Property*, NAT'L. L.J., June 9, 1997, at B5; *see also* NAT'L L. J. ONLINE (visited Nov. 19, 1999) <http://www.ljextra.com/nlj/>.

[65]. *See id*.

[66]. *See id*.

[67]. *See* F. Lawrence Street & Mark P. Grant, LAW OF THE INTERNET 382 (2000 ed.).

[68]. *See* Charlotte Waelde, *Domain Names* and *Trade Marks: What's in a Name*, *in* LAW & THE INTERNET: REGULATING CYBERSPACE 45-46 (Lilian Edwards & Charlotte Waelde eds., 1997).

[69]. *See* Avery Dennison Corp. v. Sumpton, 999 F. Supp. 1337 (1998) *rev'd and remanded* 51 U.S.P.Q.2d 1801 (1999) (noting that defendants have registered over 12,000 domain names with the hope of making money by selling the names to others); *see also* Oppedahl & Larson, LLP, *Brief of Amicus Curiae* (visited February 1, 2000) <http://www.patents.com/avery/avery1.htm>.

[70]. *See id*. (defining cybersquatter as one who registers and then "squats" on all of the accepted meanings of the domain name seeking to later sell the name to a person interested in using the domain name); *see also International Reports: India--Yahoo! Sues "Cybersquatters,"* NAT'L L.J., Mar. 8, 1999, at A12 (noting that Yahoo! obtained a temporary injunction keeping an Indian company from operating a site called Yahooindia offering India-related information and services).

[71]. *See* Intermatic, Inc. v. Toeppen, 947 F. Supp. 1227, 1230 (N.D. Ill. 1996) (listing a sample of the 240 domain names registered by the defendant).

[72]. 999 F. Supp. 1337 (C.D. Cal. 1998) *rev'd and remanded*, 51 U.S.P.Q.2d 1801 (1999).

[73]. *See id*. at 1338.

[74]. *See Intermatic*, 947 F. Supp. at 1236 (holding that defendant's registration and use of "intermatic.com" as a domain name violated the anti-dilution portion of the Lanham Act "because it lessens the capacity of a famous mark, Intermatic, to identify and distinguish goods or services as a matter of law); Panavision Int'l v. Toeppen, 938 F. Supp. 616 (C.D. Cal. 1996) (finding Illinois defendant to be subject to personal jurisdiction in California because he registered names belonging to plaintiff's business as domain names, thus harming plaintiff whose principal place of business is in California).

[75]. *See* Carl Oppedahl, *Analysis and Suggestions Regarding NSI Domain Name Trademark Dispute Policy*, 7 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 73, 87 (1996) (describing NSI's policy for deactivating domain names identical to registered trademarks upon letter from trademark holder).

[76]. *See id*. (noting that NSI would deactivate a domain name thirty days after receiving a letter from a registered trademark owner stating that the owner's trademark was identical to the domain name).

[77]. *See id*. at 89 (stating that trademark holders used NSI's deactivation policy to "win cases they could never have won in court").

[78]. Carl Oppedahl, *Pursuing Domain Name Registrants Can Backfire*, NAT'L L.J., Apr. 26, 1999, at B6 (citation omitted).

[79]. *See* W. Scott Petty, *New Proposed Rules For Resolving Domain Name Disputes*, INTELL. PROP. TODAY, June 1999, at 37; *see also Final Report of the WIPO Internet Domain Name Process* (last modified Apr. 30, 1999) <http://wipo2.wipo.int/process/eng/final_report.html>(recommending procedures for resolving domain name disputes).

[80]. *See Final Report of the WIPO Internet Domain Name Process* (last modified Apr. 30, 1999) <http://wipo2.wipo.int/process/eng/final_report.html>.

[81]. *See* Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56; Child Online Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2861. These statutes may be found at *Thomas - U.S. Congress on the Internet* (visited Feb. 5, 2000) <http://thomas.loc.gov/cgi-bin/query/z?c105:h.r.3783.eh:>.

[82]. *See* 47 U.S.C. § 223 (repealed 1997).

[83]. *See* 65 U.S.L.W. 3641 (U.S. Mar. 25, 1997) (reporting that during the oral argument on the constitutionality of the CDA, the Deputy Solicitor General responded affirmatively to Justice Breyer's question of whether high school students discussing sexual experiences online may be guilty of a felony as long as the communications were patently offensive).

[84]. *See* ACLU v. Reno, 521 U.S. 844 (1997).

[85]. Pub. L. No. 105-277, 112 Stat. 2861 (1998).

[86]. *See* ACLU v. Reno, 1998 U.S. Dist. LEXIS 18546 (E.D. Pa. 1998) (granting a temporary restraining order); ACLU v. Reno, 31 F. Supp.2d 473 (E.D. Pa. 1999) (granting a preliminary injunction).

[87]. *See, e.g.*, Jonathan Wallace & Mark Mangan, SEX, LAWS, AND CYBERSPACE xii (1997) (noting that materials that are legal off the Internet are being banned online through laws such as the CDA); Mike Godwin, CYBER RIGHTS (1998) (criticizing the trend of extending the limits of Internet regulation).

[88]. 47 U.S.C. § 230 (Supp. 1997).

[89]. *See* Stratton Oakmont, Inc. v. Prodigy Serv. Co., 23 Media L. Rep. 1794 (Sup. Ct. N.Y. 1995) (finding Prodigy to be publisher of defamatory content because Prodigy exercised control over content posted on its bulletin board).

[90]. *See* Zeran v. America Online, Inc., 958 F. Supp. 1124, 1134, *aff'd*, 129 F.3d 327 (4th Cir. 1997 (describing congressional intent in passing the immunity provision of the CDA as encouraging service providers to find ways to block or delete objectionable material before it reached schools and homes).

[91]. *See Zeran*, 958 F. Supp. at 1137 (holding that "the CDA preempts a negligence cause of action against an interactive computer service provider arising from that provider's distribution of allegedly defamatory material provided via its electronic bulletin board"); Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998) (finding that CDA granted immunity to AOL for Drudge's allegedly defamatory statements).

[92]. *See* Doe v. America Online, Inc., 718 So.2d 385 (Fla. App. 1998) (granting immunity to AOL for sexual predator's chat room marketing of videotape of sexual activity with plaintiff's young son).

[93]. *See* Ian C. Ballon, *Defamation and Preemption Under the Telecommunications Act of 1996: Why the Rule in* Zeran v. America Online *is Wrong*, 2 CYBERSPACE LAWYER 6 (July/Aug.1997) (including a critique of the decision in *Zeran* and a general criticism of 47 U.S.C. §230).

[94]. *See* Victor H. Polk, Jr., *ISP Immunity Gives Little Recourse for the Defamed*, NAT'L L.J., Apr. 26, 1999, at B8 (noting that online authors may be hard to find making it difficult for victims to pursue a defamation case).

[95]. Pub. L. No. 105-304, 112 Stat. 2860 (1998).

[96]. *See id*. (referring to Title II: Online Copyright Infringement Liability Limitation).

[97]. *See* Semiconductor Chip Protection Act of 1984, Pub. L. No. 98-620, 98 Stat. 3347 (Title III) codified at 17 U.S.C. §§ 901-914 (1994 & Supp. 1998).

[98]. 523 U.S. 135 (1998).

[99]. David A. Gerber & David Bender, *Gray Market Becomes Less of an IP [Intellectual Property] Gray Area*, NAT'L L. J., Oct. 19, 1998, at C19.

[100]. *See* Michael L. Brody & Darren C. Baker, *Trademarks May Thwart Gray Market Importers: Manufacturers Hurt by Recent Supreme Court Copyright Ruling May Turn to Trademark Laws*, NAT'L L. J., May 18, 1998, at C6.

[101]. *See Managing Exports Miscellany*, MANAGING EXPORTS, Feb. 1999, at 8; *see also* IOMA's Management Library (visited February 1, 2000) <http://www.ioma.com>.

[102]. *See* INFO. INFRASTRUCTURE TASK FORCE, INTELL. PROP. AND THE NAT'L INFO. INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELL. PROP. RIGHTS 183-94 (1995) [hereinafter White Paper], *infra* note 122.

[103]. 93 Civ. 8153 (S.D.N.Y. filed Nov. 29, 1993) (settled Nov. 7, 1995).

[104]. *See* Richard Raysman & Peter Brown, *Internet Copyright Developments*, N.Y. L. J. Jan. 9, 1996, at 3.

[105]. *See* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996) (examining the constitutionality of digital monitoring of individual reading habits looking for copyright infringement in cyberspace); Neil Weinstock Netanel, *Copyright and a Democratic Civil Society*, 106 YALE L. J. 283 (1996) (presenting a conceptual framework for copyright emphasizing "that copyright is in essence a state measure that uses market institutions to enhance the democratic character of civil society"). *Id*. at 288; Michael J. Meurer, *Price Discrimination, Personal Use and Piracy: Copyright Protection of Digital Works*, 45 BUFFALO L. REV. 845 (1997) (arguing that the policies outlined in the White Paper will result in price discrimination); Neil Smith & Andrew V. Smith, *Technical Protection Devices and Copyright Law*, 3 B.U. J. SCI. & TECH. L. 7 (1997) (discussing the sufficiency of the combination of technical devices and copyright laws to protect copyright owner's rights).

[106]. *See* Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (Section 103: Copyright Protection Systems and Copyright Management Information).

[107]. The final draft of the Internet Ad Hoc Committee recommendations can be found at *Final Report of the International Ad Hoc Committee: Recommendations for Administration and Management of gTLDs* (last modified Feb. 4, 1997) <http://www.iahc.org/draft-iahc-recommend-00.html>; *see also*, Rebecca W. Gole, *Playing the Name Game: A Glimpse at the Future of the Internet: Domain Name System*, 51 FED. COMM. L. J. 403 (1999) (examining the Internet Ad Hoc Committee's proposals and presenting suggested changes necessary for the successful overal of the domain name assignment system); Alexander Gigante, *Blackhole in Cyberspace: The Legal Void in the Internet*, 15 J. MARSHALL J. COMPUTER & INFO. L. 413 (1997); David B.

Nash, *Orderly Expansion of the International Top-Level Domains: Concurrent Trademark Users Need a Way Out of the Internet Trademark Quagmire*, 15 J. MARSHALL J. COMPUTER & INFO. L. 521 (1997).

[108]. *See* April Mara Major, *Internet Red Light Districts: A Domain Name Proposal for Regulatory Zoning of Obscene Content*, 16 J. MARSHALL J. COMPUTER & INFO. L. 21 (1997) (proposing a ".obs" or ".sex" domain for obscene material that could be easily screened by software and constitutionally sound as zoning laws are for "red light" districts).

[109]. *See* Reno v. ACLU, 521 U.S. 844, 886 (1997) (O'Connor, J., concurring in part and dissenting in part).

[110]. *See* Gole, *supra* note [two before], at 422-23; Dan L. Burk, *Trademarks Along the Infoban: A First Look at the Emerging Law of Cybermarks*, 1 RICH. J.L. & TECH. 1, ¶68 (Apr. 10, 1995) <http://www.richmond.edu/jolt/v1i1/burk.html> (noting that the increase in unsophisticated consumers may affect domain name discrimination due to the likelihood of consumer confusion with similar domain names).

[111]. A detailed description of the problem and policymaking process that eventually culminated in the passage of legislation protecting the rights of children online is documented in Tomas A. Lipinski & Elizabeth Buchanan, *Following the Piper from Hamlin: The Loss of Childhood and the Impact of Marketing and Technology* (1998) (paper presented at Computer Ethics: A Philosophical Enquiry [sic] (CEPE'98), London School of Economics and Political Science, London, United Kingdom, (In Association with the ACM SIG on Computers and Society), Dec. 14-15, 1998 (publication forthcoming by the University of London) (manuscript, on file with author).

[112]. *See* Michael Freeman, THE MORAL STATUS OF CHILDREN: ESSAYS ON THE RIGHTS OF THE CHILD (1997); Geraldine Van Bueren, THE INTERNATIONAL LAW ON THE RIGHTS OF THE CHILD (1995).

[113]. *See* Tomas A. Lipinski, *Towards a New Vision of Children in the Coming Millennium: A Childhood Manifesto for the Consumer Age*, J. INFO. ETHICS (1999) (publication forthcoming) (manuscript on file with author).

[114]. *See* In the Matter of GeoCities, Proposed Consent Agreement, 63 Fed. Reg. 44,624 (1998) (finding GeoCities committed unfair and deceptive trade practices law by falsely representing how consumers' personal information would be used).

[115]. *See* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS (1998) (recommending that Congress enact legislation protecting children's online privacy).

[116]. Public Law 105-277, 112 Stat. 2861-728 (1998) (including parental opt-out, parental notice and opt-out for children thirteen to sixteen years-old, and parental consent and opt-in for children twelve years-old and under).

[117]. *See* Arlene Bielefield & Lawrence Cheeseman, TECH. AND COPYRIGHT LAW: A GUIDEBOOK FOR THE LIBRARY, RESEARCH AND TEACHING PROFESSIONS 139-44 (1997) (discussing draft guidelines for distance learning created by the Conference on Fair Use).

[118]. *See* Laura N. Gasaway, *Universities, Libraries and Fair Use in the Digital Age*, *in* CURRENT LEGAL ISSUES IN PUBLISHING 69, 76-77 (A. Bruce Strauch, ed., 1996) (discussing copyright issues relating to distance learning); *see also*, Tomas A. Lipinski, Application of Copyright Law to Distance Education, Testimony and Written Comments, United States Copyright Office Field Hearings: Copyright Office Study on Distance Education, Feb. 12, 1999, Chicago, Illinois, Library of Congress, Copyright Office, Docket No. 99-12A, Promotion of Distance Education through Digital Technologies, Request for Comments and Notice of Public Hearing, *available at* 63 Fed. Reg. 71,167 (1998). U.S. Copyright Office Notice, *available at*

<http://lcweb.loc.gov/copyright/disted/>; Tomas A. Lipinski, *In Defense of the Right to Read and Browse Copyrighted Material or An Argued Application of Copyright Law to Distance Education: Principles, Problems and Potentials* (publication forthcoming) (manuscript on file with the author).

[119]. *See* Peter Huber, LAW AND DISORDER IN CYBERSPACE: ABOLISH THE FCC AND LET COMMON LAW RULE THE TELECOSM 199-206 (1997) (arguing that, "[l]eft to common law, the telecosm will become again a place of vast freedom and abundance"). *Id*. at 206.

[120]. *See* Brian M. O'Connell, *Private Creation of Internet "Law": Overcoming a False Intellectual Universe*, IEEE TECH. & SOC'Y, Spring, 1999, at 4 (examining philosophies of "recasting law in a digital image"). *Id*.; Ejan Mackaay, *The Economics of Emergent Property Rights on the Internet, in* THE FUTURE OF COPYRIGHT IN A DIGITAL ENVIRONMENT 13 (P. Bernt Hugenholtz ed., 1996) (questioning whether intellectual property rights work on the Internet and concluding that "even if fencing techniques crystallised in the exting copyright law do not work very well on the Internet, property is by no means dead and the net is buzzing with initiatives exploring alternative fencing techniques and new extensions of property rights"). *Id*. at 25.

[121]. *See* Kent D. Stuckey, INTERNET AND ONLINE LAW §4.03[4] (1999) (discussing international transmission of obscene material).

[122]. *See* White Paper, *supra* note 102, at 183-94.

[123]. ACLU v. Reno, 929 F. Supp. 824, 844 (1996), *aff'd sub nom*. 521 U.S. 844 (1997); ACLU v. Reno, 31 F. Supp.2d 473 (E.D. Pa. 1999).

[124]. *See* Jerry Ashworth, *Businesses Warned: Prepare for 'Cybersmear" Campaigns*, TELELCOM & DATA NETWORK SECURITY (Apr. 6, 1999) (discussing online smear campaigns directed towards businesses), *available at* <http://www.tr.com/tronline/rec/1999/re040699/re040699.htm>.

[125]. *See* Friedrich Kessler, *Contracts of Adhesion--Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629 (1943).

[126]. *See* Susan D. Rector, *E-Comerce Update: Clickwrap Agreements: Are They Enforceable?*, 13 CORP. COUNS. 1 (Mar. 1999) (defining shrinkwrap licenses as "contracts whose terms of use are printed inside the software product package" and noting the complete terms of the contract often are not known until after the consumer makes the purchase). *Id*.

[127]. *See* Ticketmaster Corp. v. Microsoft, Inc., First Amended Complaint, No. 97- 3055, (C.D. Cal. filed May 9, 1997), *available at* <http://www.ljx.com/LJXfiles/ticketmaster/complaint.html> (alleging Microsoft violated state and federal unfair competition laws by linking on an internal Ticketmaster webpage bypassing Ticketmaster's ad-filled homepage). The case resulted in a settlement on January 22, 1999.

[128]. For applying network analysis to the Internet, *see* Scoot E. Flick, *Monopolization of the 'Net? Applying a 'Network Externalities' Analysis to the Backbone Capacity of Merging ISPs, Antitrust Officials Force a Huge Divestiture*, NAT'L L. J., Nov. 9, 1998, at B5.

[129]. *See* Brookfield Comm. Inc. v. West Coast Ent. Corp., 174 F.3d 1036 (9th Cir. 1999) (concluding that a Network Solutions, Inc. domain name registration does not per se establish trademark priority, traditional trademark analysis will apply and potentially override a domain registration).

[130]. *See generally* Llewellyn Joseph Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 CORNELL J.L. & PUB. POL'Y

475, 476 (1997) (marking the "closing of the electronic frontier" as a "new age in cyberspace and the formal recognition of a post-industrial, post-service, global information driven economy"). *Id*.

[131]. *See generally* Sonya Salamon, *Cultural Dimensions of Land Tenure in the United States*, *in* WHO OWNS AMERICA? SOCIAL CONFLICT OVER PROPERTY RIGHTS 159, 159 (Harvey M. Jacobs ed.) (1998) (examining how land-tenure systems "emerged as part of the local cultural system"). *Id*.

[132]. *See generally* Paul Mungo & Bryan Clough, APPROACHING ZERO: THE EXTRAORDINARY UNDERWORLD OF HACKERS, PHREAKERS, VIRUS WRITERS, AND KEYBOARD CRIMINALS (1992) (exploring the activities of computer hackers).

[133]. *See* Ejan MacKaay, *The Economics of Emergent Property Rights on the Internet*, *in* THE FUTURE OF COPYRIGHT IN A DIGITAL ENVIRONMENT 13, 18 (P. Bernt Hugenholtz ed., 1996) (stating "[b]ut the Internet amplifies the corrosion of the older fences and creates the appearance of an open field in which all take whatever they can click their mouse on."). *Id*.

[134]. *See* I. Trotter Hardy, *The Ancient Doctrine of Trespass to Web Sites*, J. ONLINE L. art. 7 at ¶¶ 23, 48, 57 (Oct. 1996) (considering a website owner's action for trespass as an enforcement mechanism to limit access to the owner's website).

[135]. *See* David M. Mirchin, *Intellectual Property*, CORP. LEGAL. TIMES, Oct. 1998, at 22 (discussing the controversy over a newspaper's framing a link to a competitor newspaper's stories).

[136]. *See generally* CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1017 (S.D. Ohio 1997) (holding that defendants engaged in a form of trespass to personal property where defendants transmitted a large volume of unsolicited e-mail to the plaintiff's computer in spite of repeated requests to cease the practice); Cyber Promotions, Inc. v. American Online, Inc., 948 F. Supp. 436 (E.D. Pa. 1996) (finding that a private online service has the right to block unsolicited e-mail solicitations from reaching the online service's customers); Hotmail Corp. v. Van$ Money Pie, Inc., 47 U.S.P.Q. 2d 1020, 1023-24 (N.D. Cal. 1998) (enjoining defendant's transmission of bulk e-mails because defendants trespassed on Hotmail's property by using Hotmail account's in violation of Hotmail's Terms and Services and by filling up Hotmail's computer storage space with junk e-mail); Earthlink Network, Inc. v. Cyber Promotions, Inc., No. BC 167502 (L.A. Sup. Ct. 1997) (filed Mar. 13, 1997) (seeking to enjoin defendant's transmission of unsolicited e-mail advertisements); Parker v. C.N. Enterprises, No. 97-96373 (D. Tex. 1997) (Final Judgment) (finding that defendant's action constituted trespass where defendant transmitted unsolicited e-mails with a false electronic return address), *available at Parker v. C.N. Enterprises Order* (visited Oct. 25, 1999) <http://legal.web.aol.com/decisions/dljunk/parkero.html>.

[137]. For the application of the Computer Fraud and Abuse Act, 18 U.S.C. §1030 (1994 & Supp. 1998), *see*, for example, Cyber American Online v. LCGM, Inc., 46 F.Supp.2d 444 (E.D. Va. 1998) (finding that website operators' use of AOL membership to obtain e-mail addresses of AOL's customers to send bulk e-mail to those customers violated the Computer Fraud and Abuse Act's prohibition of individuals exceeding their authorized access); Hotmail Corp. v. Van$ Money Pie, Inc., 47 U.S.P.Q. 2d 1020 (N.D. Cal. 1998) (finding that plaintiff will likely prevail on plaintiff's claim that defendant violated the Computer Fraud and Abuse Act by sending bulk e-mail with falsified e-mail addresses that would tie up plaintiff's computer system); Promotions, Inc. v. America Online, Inc., 948 F. Supp. 436 (E.D. Pa. 1996).

[138]. *But see* Paul A. David, *Intellectual Property Institutions and the Panda's Thumb: Patents, Copyrights, and Trade Secrets In Economic Theory and History*, *in* NAT'L RES. COUNCIL, GLOBAL DIMENSION OF INTELL. PROP. RIGHTS IN SCI. AND TECH. 19, 29 (1992) (discussing three options: patronage, procurement and property based governance).

[139]. *See generally,* Garrett Hardin, *The Tragedy of the Commons*, 162 SCI. 1243,1246,1248 (Dec. 13, 1968) (discussing how moral, not technical, solutions are needed for problems relating to a class of human problems, such as population overgrowth).

[140]. *See* Robert Kline, *Freedom of Speech on the Electronic Village Green: Applying the First Amendment Lessons of Cable Television to the Internet*, 6 CORNELL J. L. & PUB. POL'Y 23, 39-40 (1996) (analogizing cable television to traditional public fora).

[141]. *See generally* Edward J. Naughton, *Is Cyberspace A Public Forum? Computer Bulletin Boards, Free Speech and Action*, 81 GEO. L. J. 409, 419 (1992) (noting that advocates of a First Amendment right of access to the public message areas argue that the bulletin boards "are the modern day equivalents of the streets, parks, and commons of the eighteenth century town . . ."). *Id.*; Noah D. Zatz, *Sidewalks in Cyberspace: Making Space for Public Forums in the Electronic Environment*, 12 HARV. J. L. & TECH. 149, 200-19 (1998) (reviewing attempts to create a public forum doctrine for the Internet); Steven G. Gey, *Reopening the Public Forum-From Sidewalks to Cyberspace*, 58 OHIO ST. L. J. 1535, 1537, 1618-34 (1998) (applying public forum doctrine to issues involving the Internet).

[142]. *See* David J. Goldstone, *A Funny Thing Happened on the Way to the Cyber Forum: Public vs. Private in Cyberspace Speech*, 69 U. COLO. L. REV. 1, 21 (1998) in which Mr. Goldstone states,

> [t]hus, taking the position that an Internet forum should be treated as a state actor based on an analogy to a shopping mall would not obtain for that cyber forum the 'public forum' status coveted by the free speech proponents. Such a position might highlight the extent to which Internet forums do not provide the streets, sidewalks, or other open areas that are a integral part of many shopping malls and that are also the indicia of traditional public forums under the formal doctrine. Therefore, a shopping mall analogy, though instructive, would not likely be a fruitful line of argument for the advocate seeking a right of access to a cyber forum.

Id. (citations omitted).

[143]. *See* Reno v. ACLU, 521 U.S. 844, 853 (1997) (finding that the Web is "comparable, from the readers' viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services"). *Id.*

[144]. *See, e.g.*, Child Online Protection Act, 47 U.S.C.A. § 231, *citing* Congressional Findings, Pub.L. No. 105-277, 112 Stat. 2681-736 (indicating a need to prohibit the distribution of material over the Web that is harmful to minors).

[145]. For example, in Chaplinsky v. New Hampshire, 315 U.S. 568, 571-72 (1942), the Court stated,

> it is well understood that the right of free speech is not absolute at all times and under all circumstances. There are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which has never been thought to raise any Constitutional problem. These include the lewd and obscene, the profane, the libelous, and the insulting or 'fighting' words--those which by their very utterance inflict injury or tend to incite an immediate breach of the peace.

Id. (citations omitted).

[146]. 354 U.S. 476 (1957).

[147]. *Id.* at 484.

[148]. *See* Alain Gardrat, *Current European Internet Law: Emerging Legal Issues*, 16 No. 8 CABLE TV & NEW MEDIA L. & FIN. 1, 1 (1998) (stating "[t]he Internet is here to stay. That is because it is fifty percent about sex, forty percent about business and ten percent about culture or information on communications."). *Id*. In the United States, approximately 28,000 adult websites generate close to $925 million in annual revenues. *See* H.R. REP. No. 105-775, at 8 (1998), *available at Thomas - U.S. Congress on the Internet* (visited Jan. 11, 2000) <ftp://ftp.loc.gov/pub/thomas/cp105/hr775.txt>. According to some estimates almost seventy percent of U.S. Web traffic in 1998 consisted of adult-oriented material. In 1996, close to fifty percent of all U.S. Web content was either adult-oriented or otherwise unsuitable for children. *See id*. at 10.

[149]. This editing process can also impact quality in the context of the World Wide Web. For example, in championing the beneficial role of traditional West print reporters and Westlaw-based cases, West Group promotional material cautions researchers against reliance on unedited (read inaccurate) opinions on the World Wide Web.

[150]. *See, e.g*., Orrin E. Klapp, OVERLOAD AND BOREDOM: ESSAYS ON THE QUALITY OF LIFE IN THE INFO. SOCIETY 1, 1-3 (1986) (noting that "[t]he information society is . . . susceptible to its own kinds of boredom, resulting from degradation of information in two ways, redundancy and noise, which outstrip the 'slow horse' of meaning"). *Id*. at 1; William R. Paulson, THE NOISE OF CULTURE: LITERARY TEXTS IN A WORLD OF INFO. 67-68 (1988) (defining noise as "anything that arrives as part of a message, but that was not part of the message when sent out, can be considered as noise introduced in transmission"). *Id*. at 67.

[151]. *See generally* Jonathan R. Cole & Stephen Cole, SOCIAL STRATIFICATION IN SCIENCE 216 (1973) (analyzing citation behaviors to test the hypothesis that "'experimental science has progressed thanks in great part to the work of men astoundingly mediocre, and even less than mediocre'"). *Id*. (quoting J. Ortega Y. Gasset, THE REVOLT OF THE MASSES 84-85 (1932); Heidi Lee Hoerman & Carole Elizabeth Nowicke, *Secondary and Tertiary Citing: A Study of Referencing Behavior in the Literature of Citation Analysis Deriving from the Ortega Hypothesis of Cole and Cole*, 65 LIBR. Q. 415 (1995) (examining the use of citations taken from a publication without checking the documents referenced in the cites).

[152]. *See* Arthur McEvoy, *Market and Ethics in United States Property Laws*, *in* WHO OWNS AMERICA? SOCIAL CONFLICT OVER PROPERTY RIGHTS 94, 99 (Harvey M. Jacobs ed., 1998) (stating "[p]roperty and ownership are legal concepts rooted in social institutions. They refer not simply to material objects but to the relation between individuals and society that govern material objects"). *Id*.; Ejan Mackaay, *The Economics of Emergent Property Rights on the Internet*, at 15, *in* THE FUTURE OF COPYRIGHT IN A DIGITAL ENVIRONMENT 13 (P. Bernt Hugenholtz ed., 1996) (asserting "[p]roperty rights are an essential element in a legal system supporting a market economy."); J. H. Reichman & Jonathan A. Franklin, *Privately Legislated Intellectual Property Rights: Reconciling Freedom of Contract with Public Good Uses of Information*, 147 U. PA. L. REV. 875, 884-86 (1999). Reichman and Franklin note that,

> intellectual property law has always recognized the dual function of information as both a potential object of protection under specific conditions and as the building block of knowledge hat remained unprotectable under ordinary circumstances. In one dimension, entrepreneurs bundle information into goods that compete on the general products market with or without intellectual property protection. . . When, . . . larger "grain-size" information goods attract legal protection as patentable inventions or copyrightable works of authorship, qualifying creators are rewarded with exclusive property rights that limit specified competing uses. . . ."

Id. (citations omitted).

Reichman and Franklin examine Article 2B of the U.C.C. noting that, "today's most commercially valuable information goods often fit imperfectly within the classical patent and copyright paradigms . . .A . . dominant

response is to enact new, hybrid intellectual property rights, based on modified patent and copyright principles." *Id*. at 889-90 (citations omitted); Deborah G. Johnson, Computer Ethics in the 21st Century (paper presented at ETHICOMP 99, Fourth International Conference on the Social and Ethical Impacts of Information and Communication Technologies, LUISS Guido Carli University, Rome, Italy, Oct. 6-7, 1999) (indicating that one of two major ethical challenges in the new millennium is the issue of jurisdiction in cyberspace, the other is trust) (unpublished manuscript, currently on file with author).
