Cornell Journal of Law and Public Policy

Volume 6
Issue 3 *Spring 1997*

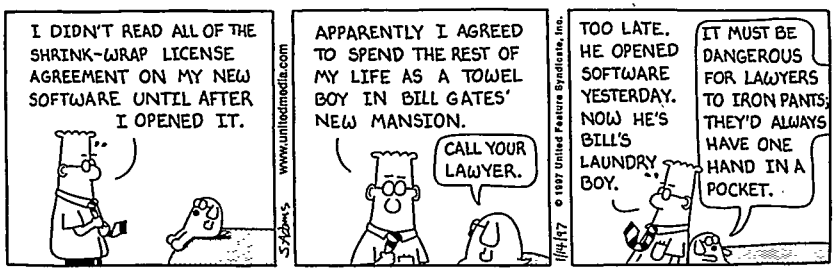
Article 1

No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace

Llewellyn Joseph Gibbons

NO REGULATION, GOVERNMENT REGULATION, OR SELF-REGULATION: SOCIAL ENFORCEMENT OR SOCIAL CONTRACTING FOR GOVERNANCE IN CYBERSPACE

Llewellyn Joseph Gibbons†



Reprinted with permission.

I. INTRODUCTION

"Cyberians"[1] are present at the creation of the jurisdiction of cyberspace and at the closing of the electronic frontier.[2] The concept of the

---

† Assistant Professor, University of Orlando School of Law. B.A. 1988, State University of New York, The College at New Paltz; J.D. 1991, Northeastern University School of Law; LL.M. 1996, Temple University School of Law. The author would like to thank Ms. Theresa McMahon for her comments on drafts of the article; Ms. Terri-Ann Gomez, the faculty secretary at the University of Orlando School of Law, for her assistance in the preparation of this article; and Charles and Olga for their encouragement. The author would like to thank the editors and staff of the Cornell Journal of Law and Policy for their patience and for allowing him to revise this article shortly before it went to press. This Article stems from Professor Gibbons's participation in the 1996 *Cornell Journal of Law & Public Policy* Symposium: *Regulating Cyberspace: Is Censorship Sensible?* (Apr. 12-13, 1996). E-mail address: <LGibbons@counsel.com>.

1 *See* Part II for a general definition and discussion of Cyberia. "Cyberians, as a general rule, dislike capital letters, which require an additional stroke on the keyboard." Robert L. Dunne, *Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace through a Contract Law Paradigm*, 35 JURIMETRICS J. 1, 3 n.6 (1994). This article will conform to this convention.

2 *See id.* at 10; HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY—HOMESTEADING ON THE ELECTRONIC FRONTIER 5 (1993); Daniel F. Burton, *The Brave New Wired World*, 106 FOREIGN POLICY 22, 36 (1997) ("The Internet is already home to a kind of Wild West ethos that is often associated with new frontiers. It is antiauthoritarian, vehement in its defense of individualism and free speech, radical in its concern with privacy, and, for the most part extremely antigovernmental.").

frontier has been a seminal one in the history of the United States, and some scholars argue the defining one.[3] Historian Frederick Jackson Turner contended that the closing of the Western expansion of the United States marked the second age of the United States. So too does the closing of the electronic frontier mark a new age in cyberspace and the formal recognition of a post-industrial, post-service, global information driven economy. For example, as early as 1978, "more than 51% of the U.S. work force was employed in areas relating to information technology earning 47% of the Gross Domestic Product (GNP)."[4] "[T]aking into account all aspects of the information industry section, the total [recently] accounted for over 65 percent of the gross national product of this country."[5] Cyberspace represents the *future* of the information industry. As the closing of the Western frontier was marked by increasing federal regulation of the West so too does closing the frontier that is cyberspace. But the frontier experience, at least in the United States, had one positive effect, the devolution of political power from Washington to the new jurisdictions, called states, that were carved out of the frontier.[6] In cyberspace, the Communications Decency Act was viewed by many as merely the first of many national attempts to impose regulation from without—the real world—and the formal beginning of a closed frontier.

A. CYBERSPACE IN A STATE OF NATURE?

Some commentators have espoused the myth of a free and unregulated cyberspace:

> [i]n the world of Cyberspace . . . anarchy reigns. There is no regulatory body, and computer users are capable of anything. The Internet is a place where everyone is welcome, regardless of gender, age, race, or association. . . . Since there is no regulatory body policing the Internet, the extent to which an individual is capable of [acting] without restriction is an enigma.[7]

---

[3] *See generally* FREDERICK JACKSON TURNER, THE SIGNIFICANCE OF THE FRONTIER IN AMERICAN HISTORY (1894); THE FRONTIER THESIS: VALID INTERPRETATION OF AMERICAN HISTORY? (Ray A. Billington ed., 1966).

[4] Harold M. White, Jr. & Rita Lauiria, *The Impact of New Communication Technologies on International Law and Policy: Cyberspace and the Restructuring of the International Telecommunications Union*, 32 CAL. W. L. REV. 1, 1-3 (1995) (citing JAMES R. TAYLOR & ELIZABETH J. VAN EVERY, THE VULNERABLE FORTRESS: BUREAUCRATIC ORGANIZATION IN THE INFORMATION AGE 25 (1993)).

[5] RAYMOND T. NIMMER, INFORMATION LAW § 1.04 (1997).

[6] A discussion of the effects of this process on the indigenous peoples of the West is well beyond the scope of this article.

[7] Barbara M. Ryga, Comment, *Cyberporn: Contemplating the First Amendment in Cyberspace*, 6 SETON HALL CONST. L.J. 221, 224 (1995). *See also* William S. Byassee, *Jurisdiction in Cyberspace: Applying Real World Precedent to the Virtual Community*, 30 WAKE

This is not the cyberspace that most Cyberians experience. Cyberspace is a community of 71 million individuals[8] which has so far relied on a distinct culture of shared norms and common values to control their behavior.[9] Cyberspace arose out of the academic and research communities and reflects a culture in which axioms of First Amendment jurisprudence became the dominant value.[10] Many Cyberians believe literally that "the best test of truth is the power of the thought to get itself accepted in the competition of the market,"[11] or that "the fitting remedy for evil counsels is good ones;"[12] yet, "no-one has a right to press even 'good' ideas on an unwilling recipient."[13] Although "the First Amendment is a local ordinance" in cyberspace, Cyberians throughout the world often invoke its talismanic force against those attempting to hinder free and robust speech. The Cyberian community is probably the most heterogeneous population that has ever existed.[14] The community is linguistically, culturally, economically, racially, and religiously diverse.[15] Cyberian infrastructures are constantly evolving.[16] The access providers, content providers, software developers, the telecommunications companies, and the roadbed itself, are combining in seemingly infinite permuta-

---

FOREST L. REV. 197, 199 (1995) ("It has no central governing authority; it operates by informal agreement among all users and more formal agreement by the owners of a number of large computers across the nation linked by high-speed telephone connection."). However, not everyone agrees with this position. Professor Nimmer contends that cyberspace is "over regulated." Nimmer, *supra* note 5, at ¶ 1.02[4] ("The law of 200 nations applies in cyberspace; it creates often conflicting demands and imposes values from multiple and diverse cultures onto a single environment.").

8 John S. Quarterman, *1997 Users and Hosts of the Internet and the Matrix*, MATRIX NEWS, Jan. 1997, at 1. Cyberspace is growing at almost an exponential rate, so any measurement is obsolete even before it's published. This article does not attempt to resolve the conflicting claims as to the size of cyberspace.

9 Dunne, *supra* note 1, at 8; George McMurdo, *Netiquette for Networkers*, 21 J. INFO. SCIENCE 305 (1995) (discussing the basic commandments, suggestions, and rules for behavior in cyberspace).

10 McMurdo, *supra* note 9, at 314.

11 Abrams v. United States, 250 U.S. 616, 630 (Holmes, J., dissenting).

12 Whitney v. California, 274 U.S. 357, 375 (1927) (Brandeis, J., concurring).

> [T]he peculiar evil of silencing the expression of an opinion is, that it is robbing the human race; posterity as well as the existing generation; those who dissent from the opinion, still more than those who hold it. If the opinion is right, they are deprived of the opportunity of exchanging error for truth: if wrong, they lose . . . the clearer perception and livelier impression of truth, produced by its collision with error.

JOHN STUART MILL, ON LIBERTY 18 (D. Spitz ed. 1975).

13 Rowan v. United States Post Office Dep't, 397 U.S. 728, 738 (1970).

14 Fred H. Cate, *Law in Cyberspace*, 39 How. L.J. 565, 565 (1996) ("Thirty-seven million users in 161 countries connect to each other generating 100 million e-mail messages every day.").

15 *See id.*

16 *See* James C. Goodale et al., *Panel I: The Changing Landscape of Jurisprudence in Light of the New Communications and Media Alliances*, 5 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 427 (1996).

tions.[17] Similar to the experience of living on a real frontier, as the community grows, the current informal methods of controlling behavior may have to yield to the pressures of civilization, population, and, above all, commerce.[18] The putative needs of the growing commercial sector of the Internet and the demands that it is making on governments is the greatest threat to the existing libertarian paradigm in cyberspace.

B. TAMING THE ELECTRONIC FRONTIER

Today, forces internal and external to cyberspace are taming the electronic frontier by establishing the first legal footpaths for "our" convenience. These forces, however, have no knowledge of either the vast technological, social, and commercial entity of cyberspace[19] or of the possible effects of the changes they are making. These tentative "footpaths" will define and shape the rules of the road for the evolution of cyberspace.[20] Unfortunately, the Communications Decency Act[21] is one such footprint that may in the process of "protecting" individuals in cyberspace obliterate free and robust speech. To make a frontier safe, one must tame it. In the process of taming it, one must remove all sense of danger and thus eliminate the unknown. The Communications Decency Act is also a paradigm of why government regulation is inappropriate for cyberspace. The CDA demonstrates the dangers of

---

17 *See id. See also* Cate, *supra* note 14, at 567 (observing that Internet not only crosses global boundaries, but also regulatory ones; for example, it provides content like broadcasters, carries content like the telcos, provides multiple channels like DST or cable TV, and delivers mail and many traditional publications like magazines and newspapers like the post office); Mark L. Gordon & Diana J. P. McKenzie, *A Lawyer's Roadmap of the Information Superhighway*, 13 J. MARSHALL J. COMPUTER & INFO. L. 177, 184-188 (1995); White & Lauiria, *supra* note 4, at 1-3.

18 *See* Dunne, *supra* note 1, at 8.

19 See Part V.A

20 This is not new. Each new means of communication faced its own outcries for regulation. In 15th Century Venice, authorities were worried that "[c]orrupt printed versions were driving out of the market the reliable old manuscript texts." Clary Corp. v. Union Standard Ins. Co., 33 Cal. Rptr. 486, 488 n.2 (Ct. App. 1994) (quoting BOORSTIN, THE DISCOVERS 529-30 (1983)), review denied and ordered not published (Dec. 22, 1994). Emperor Frederick II declared that contracts written on paper were invalid because parchment (sheepskin) was a more dignified medium for recording legal documents. At the turn of the century, lawyers were worried about the use of typewriters, see Benjamin Wright, The Law of Electronic Commerce: EDI, E-mail, and Internet Technology, Proof, and Liability § 3.4 n.2 (2d ed. 1996), and telegraph, *see* John Robinson Thomas, Note, *Legal Responses to Commercial Transactions Employing Novel Communications Media*, 90 MICH. L. REV. 1145, 1145 (1992) (citing WILLIAM L. SCOTT & MILTON P. JARNAGIN, A TREATISE UPON THE LAW OF THE TELEGRAPHS § 296 (1868)). Today, we know such fears are totally groundless. We know because each new communications medium had an opportunity to mature or time has subsequently proven such regulation superfluous.

21 Communications Decency Act of 1996, Pub. L. No. 104-104, § 502, 110 Stat. 133 (1996).

government regulation of cyberspace—the greatest danger is the balkanization of information (content).[22]

Current Internet regulators and infrastructure architects will not know the full effect of their tampering for decades, and future users who never experienced the wild electronic frontier will not realize what was lost. The following is an example of what a physical superhighway can do to existing communities:

> [From 1950 to 1970], Robert Moses built roads, bridges, parks and housing projects. Nothing stopped him—not politicians, community leaders, urban planners, neighborhoods. Quite the contrary: he bribed politicians, intimidated community leaders, hired the urban planners, and plowed under the community neighborhoods. Anyway, in 1955 only a reactionary Luddite would possibly oppose highway construction. The automobile was clearly the key to the future.
>
> Your imaginary trip across the Cross Bronx Expressway won't show you the thousands of people evicted from their homes, the old brownstone apartment made over, the diverse neighborhoods cleaved by noisy traffic arteries. Robert Moses did more to destroy New York City than any one individual.[23]

Similarly, we do not know what effect the information superhighway will have on the non-Cyberian communities. In cyberspace, *narrow*casting is the norm, in contrast to *broad*casting in the real world. "Television, for example has become the common culture of those who have grown up with it; it contributes to their sense of being members of a nation. . . . [S]ocial and political leaders have looked to the media to provide the social cohesion once supplied by public places."[24] Outside of cyberspace, the media serves a legitimatization function and defines the scope of public discourse. The "media" defines the terms of the debate, and which sources are authoritative. Without a common language and points of reference, public discourse is impossible. The possible effect of a world where "news" is narrowly cast is to fracture the polity into increasingly smaller communities without a common language. Other commentators have found that electronic networks facilitate political ties across traditional socioeconomic boundaries and power differen-

---

22 *See A Framework for Global Electronic Commerce* (visited July 2, 1997) <http://wwww.whitehouse.gov/WH/Commerce/read.htm> (expressing the Clinton's Administration's concern that content restrictions may become trade barriers).

23 CLIFFORD STOLL, SILICON SNAKE OIL 49 (1995).

24 PATRICK M. GARRY, SCRAMBLING FOR PROTECTION: THE NEW MEDIA AND THE FIRST AMENDMENT 4 (1994).

tials and that the network increased participation in civic life.[25] So, the effect of living in a world of free and easily obtained information and communication may weaken political bonds or tighten them. But

> [t]he evolution of information and communications technology . . . will probably heavily favor nonstate entities . . . over states. The new technologies encourage noninstitutional, shifting networks over the fixed bureaucratic hierarchies that are the hallmark of the single-voiced sovereign state. They dissolve issues' and institutions' ties to a fixed place. And by greatly empowering individuals, they weaken the relative attachment to community, of which the preeminent one in modern society is the nation state.[26]

Regardless of whether cyberspace is a broadcaster, narrowcaster, or merely a common carrier, it has the potential to produce changes in existing geopolitical, social, and cultural institutions.

Governments already have the *power* to regulate cyberspace that is coterminous with their geographical boundaries. But, it is not clear that they can effectively regulate that portion of cyberspace without denying their citizens its benefits.[27] Software that allows parents or employers to control access to sites on the Internet which they deem inappropriate may be the prototype of instruments that allow governments to censor the information available to their citizens on the net. As blocking software becomes more prevalent and sophisticated, and PICS (Platform for Internet Content Selection) and other rating systems become standard, governments may mandate that all the Internet service providers in a country install blocking software to screen for content that is offensive to the current regime.[28] This mechanism will give governments the power

---

25 Michele Andrisin Wittig & Joseph Schmitz, *Electronic Grassroots Organizing: Public Electronic Network (PEN) Actions Group*, 52 J. SOC. ISSUES. 53 (1996).

26 Jessica T. Mathews, *Power Shift*, 76 FOREIGN AFFAIRS 50, 66 (1997); but see Burton, *supra* note 2, at 37 ("[I]t will be a networked world comprised of electronic communities of commerce and culture—a world that ironically will strengthen the position of the United States as a nation among nations, even as it disrupts the system of nation-states."); Barry Wellman, et al., *Computer Networks as Social Networks: Collaborative Work, Telework, and the Virtual Community*, 22 AMER. REV. SOC. 213, 231-32 (1996) ("Social networks are simultaneously becoming more global and more local as worldwide connectivity and domestic matters intersect,. Global connectivity de-emphasizes the importance of locality for work and community; on-line relationships may be more stimulating than suburban neighborhoods and alienated offices.").

27 Timothy S. Wu, Note, *Cyberspace Sovereignty?—The Internet and the International System*, 10 HARV. J.L. & TECH. 647, 651-53, 659-60 (1997).

28 Paul Resnick, *Filtering Information on the Internet*, SCIENTIFIC AMERICAN SPECIAL REPORT (visited May 5, 1997) <http://www.sciam.com/0397issue/0397resnick.html> ("Singapore and China, for instance, are experimenting with 'national firewalls'—combinations of software and hardware that block their citizens' access to certain newsgroups and web sites.").

to censor content that previously was only imaginable in a Kafkaesque dictatorship. But the ability to impose order on cyberspace begs the question of whether a *sui generis* law of cyberspace is *really* necessary or even wise. Accordingly, denizens[29] of cyberspace must focus their attention on providing a paradigm to govern this brave new world or governance will be imposed from without.

C. FUTURE GOVERNMENT IN CYBERSPACE

Any paradigm for governing cyberspace must be flexible, yet strong enough to meet the challenges of the next century — and perhaps the indefinite future. Further, this paradigm must contain a basis for adjudicating disputes in cyberspace. The Cyberian community must accept the "law" of cyberspace as legitimate and the enforcement of these laws as just. An anarchistic self-regulating community developed Cyberian norms and values. Rights in cyberspace focus on the power to "possess" or control information. As with the real frontier, how we allocate rights in cyberspace — and how we close it — will determine how we measure justice and to whom this justice will be accorded. The existing *ad hoc* process of rule making, fact finding, adjudication, and punishment is ill-defined and amorphous. Few rules exist. Rules are established by mutual agreement, and like the old West, each person defends his or her own electronic homestead; violating the few rules that exist is punished through technology, social forces, or by system administrators. The "adjudication process," once started, is swift and unappealable. The new paradigm, however, must establish a rule making, fact-finding, adjudication, and enforcement process that is accepted as legitimate and is enforceable both in cyberspace and in the real world.

1. *Life, Liberty, and Property in Cyberspace*

In cyberspace, any division between "rights" and "property" is an artificial and false dichotomy. Many of the legal issues raised in cyberspace are traditionally intellectual property issues.[30] For example, free-

---

29 Surprisingly, there appears to be very little academic literature regarding "citizenship" in cyberspace or Cyberian communities. *But see* Henry H. Perritt, Jr., Self-Governing Electronic Communities (Apr. 2, 1995) *in* COMPUTER LAW ASSOCIATION, THE 1995 COMPUTER & TELECOMMUNICATION LAW UPDATE 59 (1995) (pagination in draft). This paper does not attempt to resolve who is a "citizen," "resident," or "tourist" in Cyberia or cyberspace. The term denizen was selected as being appropriately legally ambiguous. *See* THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 498 (3d ed. 1992) ("Denizen: (1) An inhabitant; a resident . . . (2) One that frequents a particular place . . . (4) A foreigner who is granted rights of resident and sometimes of citizenship.").

30 Professor Chon makes the point elegantly, "three men are standing at the end of a very long pipe. Instead of being circular, it is C-shaped. One of the men says, 'I'm afraid, Inspector, this means that everybody and everything in the country has been copyrighted.'" Margaret Chon, *New Wine Bursting From Old Bottles: Collaborative Internet Art, Joint Works,*

dom of speech implicates a property right in what is spoken, as speech in cyberspace is always reduced to tangible form; thus, creating a copyright (property) interest in pure speech.[31] "Property" in cyberspace is information, and "power" is the ability to control information.[32] The creation and protection of *property* is a core function of government.[33] This is especially true in cyberspace because "[w]hen contrasted with goods, information is unusual property. Economists describe it as 'public goods.' Once released, further disseminations of information cannot be prevented without the aid of law."[34]

2. *Legal Issues in Cyberspace*

The law of cyberspace must address allocating rights and responsibilities in cyberspace over:

(1) *access* — individuals not yet on cyberspace want access to the network and others presumably will want to deny them access;[35]

---

and Entrepreneurship, 75 OREGON L. REV. 257, 257 (1996) (describing a New Yorker cartoon).

31 *See* Copyrights Act of 1976 § 102(a), 17 U.S.C. § 102(a) (1994); MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511, 519 (9th Cir. 1993) (Loading software into RAM creates a copy under the Copyright Act.), *cert. denied*, 510 U.S. 1033 (1994); Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 260 (5th Cir. 1988) ("[T]he act of loading a program from a medium of storage into a computer's memory creates a copy of the program."); 2 NIMMER ON COPYRIGHT § 8.08 at 8-105 (1983) ("Inputting a computer program entails the preparation of a copy."); FINAL REPORT OF THE NATIONAL COMMISSION ON THE NEW TECHNOLOGICAL USES OF COPYRIGHTED WORKS, at 13 (1978) ("[T]he placement of a work into a computer is the preparation of a copy.").

32 Property ownership is a bundle of the legal rights of control. Property rights are not absolute. Unlike physical property (either real property or goods) which can be physically possessed, property rights in information are intangible. Numerous individuals can possess the same information. Once the secret is out, property interests in information can only be protected through statutory or contract rights. Therefore, the focus of property rights in information is control over access and dissemination of the information. *See* Raymond T. Nimmer & Patricia Ann Krauthaus, *Beyond the Internet: Settling the Electronic Frontier*, 6 STAN. L. & POL'Y REV. 25, 26-27 (1994). *See also* John Lienhard, Address *Reflections on Information, Biology, and Community*, 32 HOUS. L. REV. 303, 313-14 (1995) (suggesting the need to reconsider property rights in information); John Perry Barlow, *The Economy of Ideas: a Framework for Rethinking Patents and Copyrights in the Digital Age*, WIRED 2.03, Mar. 1994; Esther Dyson, *Intellectual Value*, WIRED 3.07, July 1995.

33 *See* James Madison, *Property*, *in* 14 PAPERS OF JAMES MADISON 266-68 (Robert A. Rutland et al. eds., 1983). *See generally* Michael Rosenfeld, *Contract and Justice: The Relations Between Classical Contract Law and Social Contract Theory*, 70 IOWA L. REV. 769 (1985) (generally discussing the role of property and the creation of the social contract as seen by John Locke, Thomas Hobbes, and Jean-Jacques Rousseau).

34 Nimmer, *supra* note 5, at ¶ 2.05 (1997) (citation omitted); *but see* Part VI.A.1.e (discussing technology based intellectual property protection).

35 Access may also include equal accommodation issues, for example an all-male or all-female listserves. *See, e.g.*, James W. Sweeney, *SRJCN Bulletin Board Scrapped Teacher Tires of Checking Computer Notes*, PRESS DEMOCRAT B1 (Feb. 11, 1995) (U.S. Department of Education ruled the separate men's and women's bulletin boards violated civil rights laws); Eugene Volokh, *Freedom of Speech in Cyberspace from the Listener's Perspective: Private*

(2) *distribution* — individuals may want to prevent information from being distributed or damages for the failure to distribute information;

(3) *contracts* — individuals want others to live up to their commitments on the net; and

(4) *torts* — defamation, libel, or assault.[36]

The question, then, becomes which form of governing cyberspace can best protect the legitimate interests of Cyberians.

3. *Models of Governance*

This article will explore three possible models for regulating cyberspace: *no regulation, government regulation,* and *self-regulation.* These models are not mutually exclusive, and much like the real world, any effective governance of cyberspace will be a mixture of all three. Ultimately, the question is the proper mixture. No government regulation is a null choice. Governments already regulate behavior, adjudicate disputes, and provide remedies for wrongs committed in cyberspace. This article advocates that before adding new levels of governance to cyberspace, governments should first determine if existing government regulation is adequate to protect government's sovereign interest in regulating cyberspace. The government's interest should be measured by the externalities of the actions in cyberspace. As the effect of the Cyberian action or inaction becomes greater in the real world so does that government's interest in regulating the action or inaction. Implicit in this model of government regulation is the principle that most regulation in cyberspace will be self-regulation. In determining the need for new regulation in cyberspace, governments should apply a cost-benefit analysis to the new regulation evaluating the costs of the existing uncertainty absent the regulation, and the costs and benefits that the proposed regulation would have on Cyberian transactions.

Self-regulation may assume many forms that range from social control to formal contracts. Much regulation in cyberspace is already done through informal social controls. This article examines the formal contract based form of government as the legitimate model for creating institutions to which governments will grant some form of autonomy. A self-regulation model based on contract law is appropriate because the contract law model, when it *represents the true meeting of the minds*, best fits the libertarian frontier traditions of cyberspace. A contract-based law

---

Speech Restrictions, Libel, State Action, Harassment, and Sex, 1996 U. CHI. LEGAL F. 377, 390-96 (1996) (discussing the right to exclude participants).

36 *See* Henry H. Perritt, Jr., *Dispute Resolution in Electronic Networked Communities*, 38 VILL. L. REV. 349, 352 (1993). At the current state of cyberspace technology, battery and other personal injury torts do not appear to be legal issues in the foreseeable future.

of cyberspace facilitates the governing of cyberspace. Contract is, in essence, private law-making. Contracts can provide for choice of law, forums, jurisdiction, and dispute resolution, thus avoiding the difficult questions of which jurisdiction's laws will govern the dispute.[37] Unlike government, contracts made in the marketplace rapidly react to changing economic, technological, or social circumstances. Yet, as in all governments (private or public), there must be effective checks on the primacy of the new social contract or Cyberians may unwittingly contract away their liberties.[38] The danger of the contract law model is that the same standard from contract that establishes the right will also specify how that right will be enforced. Cyberians must reject any attempt to shrink-wrap governance in cyberspace by imposing a standard form contract of adhesion as the model for contracting in cyberspace. Therefore, contracting in cyberspace should be the quintessential *negotiated* contract that represents a true meeting of the minds.

Ultimately, the strongest argument for self-regulation is that it works. Under the current *laissez-faire* approach, cyberspace has experienced exponential growth measured by the total number of users, total volume or dollar value of commerce, and the advancement of the technology. Further, the technology, software, and infrastructure has responded virtually instantaneously to meet every perceived need or to protect against perceived dangers. Thus, experience in cyberspace militates for a hands-off approach by government.

II. EXISTING INFRASTRUCTURE AND GOVERNANCE IN CYBERSPACE

The term *cyberspace* is used to refer to communications *via* computer networks.[39]

---

37 *See* RESTATEMENT (SECOND) OF THE CONFLICT OF LAWS § 187 (1971).

38 *See* Heinrich Kronstein, *Business Arbitration—Instrument of Private Government*, 54 YALE L.J. 36, 68-69 (1944).

39 Senator Albert Gore — later vice-president of the United States — coined the term "information superhighway" in 1978. The terms "information superhighway," "National Information Infrastructure" ("NII"), and "electronic highway" are used interchangeably. *See* Gordon &. McKenzie, *supra* note 17, at 179 nn.2-3 (1995) (citing Daniel Pearl, *Colliding Clichés and Other Mishaps on the Term Pike*, WALL ST. J., Feb. 1, 1994, at A5). Regardless of the cliché currently in vogue, the information infrastructure functions as a "seamless web of communications networks, computers, databases, and consumer electronics that will put vast amounts of information at user's fingertips. Development of the NII can help unleash an information revolution that will change forever the way people live, work, and interact with each other." Gordon & McKenzie, *supra* note 17, at 179-80 (citing White House National Information Infrastructure Agenda for Action, Sept. 15, 1993). For general discussion of the NII, see Ralph J. Andreotta, *The National Information Infrastructure: Its Implications, Opportunities, and Challenges*, 30 WAKE FOREST L. REV. 221 (1995); ACLU v. Reno, 929 F. Supp. 824, 830-31 (E.D. Pa. 1996) ("The Internet is not a physical or tangible entity, but rather a giant network which interconnects innumerable smaller groups of linked computer net-

> These methods [of accessing the Internet] are constantly evolving and difficult to categorize precisely. But, as presently constituted, those most relevant to this case are electronic mail ("e-mail"), automatic mailing list services ("mail exploders," sometimes referred to as "listservs"), "newsgroups," "chat rooms," and the "World Wide Web." All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium—known to its users as "cyberspace"—located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet.[40]

This sense of place is so great that some Internet users refer to themselves as "Cyberians" and this electronic world as "Cyberia." Cyberspace is the virtual (electronic) nexus, agora, marketplace, or town square, where activity among computer users takes place.[41] Cyberspace is the conceptual "location" of the electronic nexus between the individual, the networks, and other individuals. Cyberspace is a place "without physical walls or even physical dimensions" in which interaction occurs as if it happened in the real world and in real time; this is "virtual real-

---

works. . . . The resulting whole is a decentralized, global medium of communications — or 'cyberspace' — that links people, institutions, corporations, and governments around the world."), *aff'd* 1997 WL 348012 (1997).

40 *Reno v. ACLU*, 1997 WL 348012, *5 (U.S.).

41 *See* Dunne, *supra* note 1, at 2-3. Cyberspace is a term originally created by science fiction writer William Gibson in his short story "Burning Chrome." *See generally* William Gibson, *Burning Chrome*, 4 OMNI 72 (1982). However,

> [i]n more than one article, an author asserts that the term "cyberspace" was coined by author William Gibson in his 1984 novel *Neuromancer*. Although not far off-target, this assertion is, in fact, incorrect. Gibson did indeed coin the term, but he coined it for his 1982 short story "Burning Chrome."
>
> What may confuse the occasional law-review editor is that the story "Burning Chrome" was not published in any collection of Gibson's short stories until 1986. Nevertheless, the story itself was published two years *before Neuromancer*, and our citations should reflect this.

Mike Godwin, e-mail (May 3, 1996) <http://mailmunch.law.cornell.edu/listserves/Cyberia/1532.html>;< http://mailmunch.law.cornell.edu/listserves/Cyberia/1538.html>; and <http://mailmunch.law.cornell.edu/listserves/Cyberia/1539.html> (visited Apr. 30, 1997).

Because the term was popularized from *Neuromancer*, this article will discuss cyberspace as it exists in the world of Gibson's *Neuromancer*, in which individuals enter a different reality, "cyberspace." Computers generate a "virtual reality", where individuals physically move about in the data "matrix" to obtain information by controlling sensory stimuli. *See* Dunne, *supra* note 1, at 3. In Gibson's vision, cyberspace is a "consensual hallucination that [was experienced by the senses as] physical space but actually was a computer-generated construct representing abstract data." *Id.* at 3 n.6.

ity,"[42] the manifestation of the "words, human relationships, data, wealth, and power . . . by people using [computer-mediated communications]."[43]

Although spatial metaphors help describe the experience of living in a Cyberian community, biological metaphors may more accurately convey the reality.[44] Culturally, socially, religiously, and economically diverse communities come together so that

> the whole system is propagating and evolving, . . . Cyberspace [is] a social petri dish, the [Intern]et [is] the agar medium, and virtual communities, in all their diversity, [are] the colonies of microorganisms that grow in petri dishes. Each of the colonies of a microorganism— the communities on the [Intern]et— is a social experiment that nobody planned but that is happening nevertheless.[45]

And, it is constantly evolving. Therefore, cyberspace is an amorphous jurisdiction without geographical or territorial limits,[46] and it may best be measured by its "population," "infrastructure," and "commerce." This article adopts an operational definition of cyberspace: All communications mediums which have at least the capability of accessing the Internet and all users of such communications mediums are part of cyberspace, even if their use or access is tangential.[47] Although the nation-state may not be the best metaphor for cyberspace, this section will briefly examine measures that are typically used to evaluate a nation-state: history, demographics, infrastructure, constituent communities, government, and revenue. These establish the existing institutional, social, and economic framework that must be accommodated in any possible governance of cyberspace.

---

42 *See* Laurence H. Tribe, *The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier*, THE HUMAN., Sept.-Oct. 1991, at 15.

43 RHEINGOLD, *supra* note 2, at 5.

44 *Id.* at 6.

45 *Id.*

46 *See* Lawrence Lessig, *Constitution and Code*, 27 CUMB. L. REV. 1 (1996-97) (describing a process of cyberzoning); Reno v. American Civil Liberties Union, 1997 WL 348012, *22-24 (O'Connor, J., concurring in the judgment in part and dissenting in part)(discussing cyberzoning).

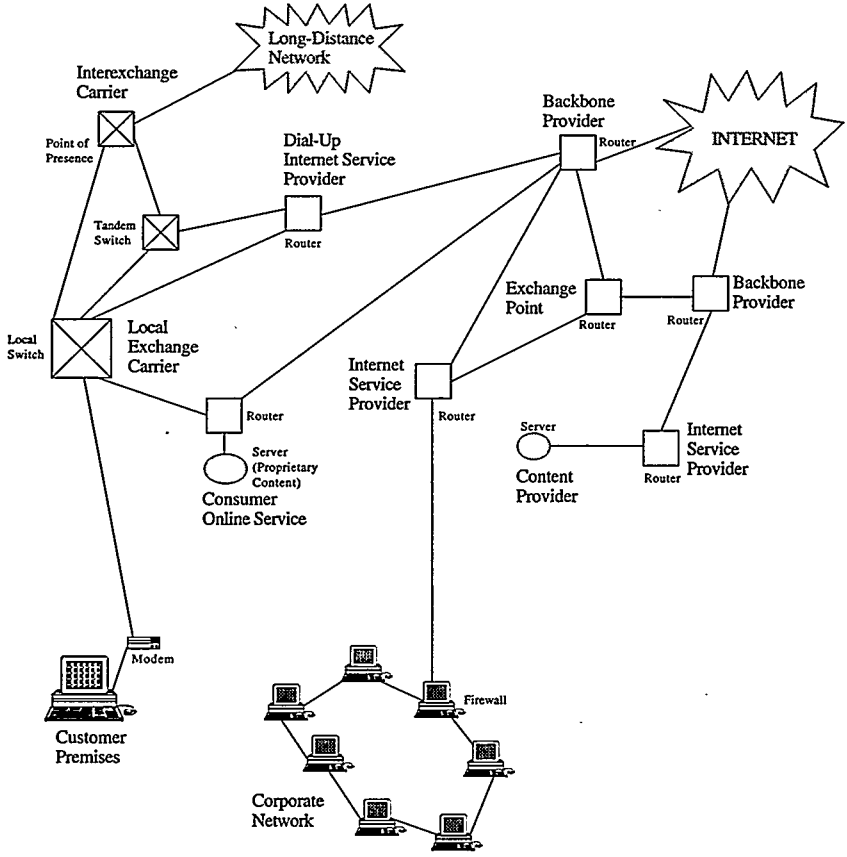
47 *Cf.* John S. Quarterman & Smoot Carl-Mitchell, *What is the Internet, Anyway?*, MATRIX NEWS 4(8), Aug. 1994 <http://www.mids.org/what.html> (defining the Internet in terms of technical specifications and access).

A. A BRIEF HISTORY OF CYBERSPACE'S MAIN STREET — THE INTERNET

The "market street" that leads to cyberspace is the Internet.[48] The Internet is a network of networks.[49] A good description of the Internet is

---

[48] As with many aspects of cyberspace, the origin of the term "Internet" is unclear. It began to be used in the early 1980s to describe the interconnection of networks to form an "internetwork." KEVIN WERBACH, DIGITAL TORNADO: THE INTERNET AND TELECOMMUNICATIONS POLICY, OFFICE OF PLANS AND POLICY, FEDERAL COMMUNICATIONS COMMISSION, OPP WORKING PAPER NO. 29, 15 n.19 (Mar. 1997). There is no statutory definition of the Internet. The 1996 Communications Decency Act for the purposes of limiting the dissemination of proscribed "indecent" content defined the Internet as "the International computer network of both Federal and non-Federal interoperable packet switched data networks." *Id.* at 12 (quoting 47 U.S.C. § 230 (1994)). See Figure 1 for a map of cyberspace. Figure 1 is reproduced with permission from KEVIN WERBACH, DIGITAL TORNADO: THE INTERNET AND TELECOMMUNICATIONS POLICY, OFFICE OF PLANS AND POLICY, FEDERAL COMMUNICATIONS COMMISSION, OPP WORKING PAPER NO. 29, 15 n.19 (Mar. 1997).



[49] RICHARD W. WIGGINS, THE INTERNET FOR EVERYONE: A GUIDE FOR USERS AND PROVIDERS 5 (1994). The Internet is described as "[t]he largest, richest, and most diverse region in cyberspace." *See also* Byassee, *supra* note 7, at 200. For an online history of the Internet, see <http://info.isoc.org/guest/zakon/Internet/History/HIT.html>; ACLU v. Reno, 929 F. Supp. 824, 830 (E.D. Pa. 1996), *aff'd* 1997 WL 348012 (1997).

controlled chaos. The Internet has no owner or central authority.[50] The unique characteristics of the Internet are its architecture and its fractal nature. The Internet's architecture minimizes the importance of physical location and classifications such as senders and receivers.[51] The Internet communicates using an adaptive system so that when one host is busy or off-line, the Internet reroutes the message. Numerous "conversations" can share the same physical facilities, and any host may communicate with any other host.[52] Because the Internet divides communications traffic into packets dedicated point-to-point connections are unnecessary.[53] The Internet has grown on an *ad hoc* basis that depended on the communications needs of the constituent networks. In 1981, the Internet was a network consisting of 300 computers.[54] Over time, more networks and users connected, forming a network of networks — the Internet. In 1989, the network consisted of over 90,000 computers.[55] Since the early 1990s, the Internet has grown into a vast commercial network where everything from software to pornography is available.[56] Today, over 9,400,000 computers comprise the network.[57] The Internet developed as part of the Advanced Research Project Network ("ARPAnet") in 1969.[58] ARPAnet was a Department of Defense initiative to assure network communications even during partial outages.[59] The ARPAnet model assumes that the network is unreliable.[60] So, the routing and delivery information is contained within the message itself.[61] To send a "message" (data) on the Internet, the server (source computer) places the message in an "envelope" (Internet Protocol (IP) packet) and then addresses the envelope. As the message travels through communicating

---

50 WIGGINS, *supra* note 49, at 5-6; CYBERSOCIETY: COMPUTER-MEDIATED COMMUNICATION AND COMMUNITY 4 (Steven G. Jones ed., 1995) ("[N]o one group manages [the Internet]. Instead, a variety of groups, such as the Internet Society and InterNIC, circulate information and resolutions and do research on the network's needs."); RIGHTS AND RESPONSIBILITIES OF PARTICIPANTS IN NETWORKED COMMUNITIES 20, 133-34 (Dorothy E. Denning and Herbert S. Lin eds., 1994) (noting the decentralized nature of the Internet).

51 Werbach, *supra* note 48, at 3.

52 *Id.*

53 *Id.*

54 ACLU v. Reno, 929 F. Supp. 830, 831 (E.D. Pa. 1996), *aff'd* 1997 WL 348012 (1997).

55 *Id.*

56 Ryga, *supra* note 7, at 223. International Data Corporation estimates that one-in-three Web surfers shops on-line. *See* Diane Trommer, *IDC Reveals the Truth About Cybershopping*, ELECTRONIC BUY'S NEWS, May 20, 1996, at 58 (Home Web shoppers spend on average $50 per month and business Web shoppers $500 per month; IDC estimated that there was $300 million in commerce on the Web in 1995 and predicts over $15 billion by the year 2000.).

57 *ACLU*, 929 F. Supp. at 831.

58 ED KROL, THE WHOLE INTERNET: USER'S GUIDE AND CATALOG 13 (2d ed. 1995); Ryga, *supra* note 7, at 223.

59 Robert Craig Waters, *An Internet Primer*, 44 FED. LAW. 33, 33-34 (1997).

60 ED KROL, THE WHOLE INTERNET USER'S GUIDE & CATALOG 15 (Academic Ed. 1995).

61 *Id.*

computers, it is routed correctly and, if necessary, rerouted based on the envelope address; this is called "dynamic routing."[62] Dynamic routing may deliver a message or even parts of the same message by taking different routes to the destination, depending on the most efficient path.[63] Efficiency is measured by the length of time it takes to deliver the message. Moreover, the routing is not geographically direct. A message sent *via* e-mail from Berkeley, California to Seattle, Washington is frequently routed: Berkeley, to Santa Clara, to Washington, D.C., to New York, to Cleveland, to Chicago, to San Francisco, to Seattle.[64] This flexibility is the Internet's greatest strength. But dynamic routing results in two potential legal problems: (1) the sender does not know what route the message will take and, consequently, what the sender's obligation to the intermediate nodes that the message passes through; and (2) the intermediate nodes handle traffic from sources they do not know.[65] The sophistication of Internet routing creates problems for localities, states, and even countries that wish to exercise jurisdiction over these transient packets.[66]

The second unique characteristic of the Internet is its "fractal nature."[67] The telecommunications industry has developed sophisticated statistical models to predict aggregate user patterns. But, these models do not accurately reflect Internet usage.[68] Internet usage does not follow the traditional "*poisson* pattern but rather a fractal distribution."[69] The "frequency of Internet connections, the distribution between short and long calls, and the pattern of data transmitted through a point on the network tend to look similarly chaotic regardless of time scale."[70] Because of the fractal nature of the Internet, existing regulatory and economic models established for other technologies are inapplicable to cyberspace.[71] Consequently, governments must be careful. Existing ex-

---

62 Perritt, *supra* note 36, at 352.

63 *Id.* at 352 n.7.

64 Joanna H. Kim, Comment, *Cyberporn Obscenity: The Viability of Local Community Standards and the Federal Venue Rules in the Computer Network Age*, 15 LOY. ENT. L.J. 415, 419 n.36 (1995).

65 *Id.* at 352. *See also* ACLU v. Reno, 929 F. Supp. 830, 831 (E.D. Pa. 1996), *aff'd* 1997 WL 348012 (1997).

66 *See, e.g.*, CompuServe v. Patterson, 89 F.3d 1257 (6th Cir. 1996); Richard S. Zembek, Comment, *Jurisdiction and the Internet: Fundamental Fairness in the Networked World of Cyberspace*, 6 ALB. L.J. SCI. & TECH. 339, 355-56 (1996).

67 Fractals are derived from the branch of mathematics known as chaos or complexity theory. Fractals exhibit "self-similarity"; in other words, a rough similar pattern emerges at any chosen level of detail." Werbach, *supra* note 48, at 3.

68 *Id.*; Herbert Snyder & Douglas Kurtze, *Chaotic Behavior in Computer Mediated Network Communication*, 32 HUMAN PROCESSING & MANAGEMENT 555, 561 (1996).

69 Werbach, *supra* note 48, at 3.

70 *Id.*

71 *See id.*

perience in telecommunications regulation may not be generalizable to cyberspace.

> [F]ractals have valuable attributes. In a fractal entity, order emerges from below rather than being dictated from above. The fact that the Internet does not have an easily-identifiable hierarchy or any clear organizational structure does not mean that all behavior is random. Many small, uncoordinated interactions may produce an aggregate whole that is remarkably persistent and adaptable.[72]

Accordingly out of the chaos on the Internet some form of order may arise — in time.[73]

In the early 1980s, the National Science Foundation (NSF) supported five regional supercomputers which were linked to research universities by NSFNET in 1986.[74] NSFNET quickly replaced ARPAnet as the back bone of the Internet.[75] NSF began the privatization of the Internet when it contracted with the Merit Network, Inc. in 1987 to run and upgrade the backbone of the Internet.[76] In 1993, the process of privatization was largely completed when NSF contracted with AT&T,[77] Network Solutions,[78] and General Atomics for basic administrative services.[79] AT&T is responsible for directory and database services (keeping track of how to locate people and resources). Network Solutions is responsible for assigning Internet addresses (thus acting as a gateway and potential choke point for) determining exactly which sites are granted permission to join the high-speed network. General Atomics is responsible for network services provided to network users (maintaining and modernizing software for using the Net). The result was Network Information Center (INTERNIC). INTERNIC was given permission to charge users other than the United States research and education communities.[80]

After the NSF announced that it would not renew Network Solutions Inc's exclusive right to allocate domain names, the International Telecommunications Union (ITU) cosponsored a conference on restruc-

---

72 *Id.*

73 *Cf.* ROBERT NOZICK, ANARCHY, STATE, AND UTOPIA (1974).

74 RHEINGOLD, *supra* note 2, at 84. For an interesting time line of the Internet's development, see Barry M. Leiner, et al., *A Brief History of the Internet*, <http://info.isoc.org/guest/Zakon /Internet/History/HIT.html>.

75 RHEINGOLD, *supra* note 2, at 84.

76 *Id.*

77 John Byczkowski, *Online Internet Watcher Tries to Uncover Every Little Nook*, CIN. ENQUIRER, Oct. 25, 1994, at B6.

78 *Id.*

79 *Id.*

80 RHEINGOLD, *supra* note 2, at 88.

turing the Internet domain name system.[81] In May 1997, the Internet Assigned Number Authority[82] (IANA) and the Internet Society (ISOC) entered into a Memorandum of Understanding on the Generic Top Level Domain Name Space of the Internet Domain Name System (gTLD-MoU).[83] The Secretary-General of the International Telecommunications Union (ITU) is the depository for the MoU.[84] The MoU requires the creation of a gTLD (Generic Top Level Domain) Policy Oversight Committee (POC).[85] In addition to the IANA, ISOC, and IAB, the ITU and World Intellectual Property Organization (WIPO) are also represented on the gTLD-POC.[86] This is implicit recognition by two major Intergovernmental Organizations (IGOs) of the unique role of the ISOC, the IAB, and the IANA. This international recognition of the ISOC, IAB, and the IANA as international players may be the first tentative steps to a unique legal status for cyberspace. Further, the ITU under § 4(c) of the MoU is obligated "to facilitate further cooperation in the implementation of [the] MoU."[87]

Under MoU, the creation of the seven generic top-level domain names was accompanied by the creation of an alternative dispute resolu-

---

81 International Telecommunication Union, Press Release (ITU/97-8) at 80, *Organizations Sign MoU to Restructure the Internet* (visited June 20, 1997) <http://www.itu.int/PPI/press/releases/1997/itu-08.htm>. NSI's contract was due to expire in 1998.

82 IANA coordinates the assignment of port and the values for options with IP/TCP and other protocols. *See* David H. Crocker, *Evolving the System, printed in*, INTERNET SYSTEM HANDBOOK 53 (Marshall T. Rose and Daniel C. Lynch eds. 1993), *quoted in* <http://www.wia.org/pub/iana.html> (for a detailed history of U.S. DoD [Internet] Assigned Numbers [Authority], Network Information Centers (NICs), Contractors, and Activities). IANA also has the authority to supervise and control the creation and management of International Top Level Domains (iTLDs). Alexander Gigante, *Blackhole in Cyberspace: The Legal Void in the Internet*, 15 J. MARSHALL J. COMPUTER & INFO. L. 413, 416 (1997).

83 *Memorandum of Understanding on the Generic Top Level Domain Name Space of the Internet Domain Name System* (gTLD-MoU) <http://www.iahc.org/gTLD-MoU.html>. Top Level Domains are indicated by, for example, *.com, .org, .edu*, or *.net*. So in the email address "user@aol.com," *AOL* is the second level domain, and *.com* is the top level domain.

84 *Id.* at § 5.

85 *Id.* at § 6.

86 *Id.* at § 6(g).

87 Unfortunately, time constraints do not permit a fuller or more considered exposition of what this unique event does and may mean for the future of cyberspace.

tion system.[88] The WIPO Arbitration and Mediation Center provides procedures for resolving commerical disputes.[89]

> [T]he WIPO Center administers procedures only. It does not set law, nor does it create substantive rules. The relevant law to be applied in the context of ADR comes from other sources, such as the relevant national or regional law. The WIPO center itself does not have jurisdiction to settle disputes, but rather to administer procedures which facilitate the settling of disputes.[90]

The WIPO Center will provide two types of alternative dispute resolution services. The WIPO Center will provide (1) traditional arbitration and mediation services, and (2) a novel procedure created by the IAHC under the MoU, "Administrative Domain Name Challenge Panels" (ACPs).[91] The ACP procedures are designed for domain name conflicts and represent a fast, inexpensive, alternative to formal judicial resolution.[92]

B. GOVERNMENT OF CYBERSPACE

Cyberspace has "evolved into a self-regulating, anarchistic community with nobody in charge."[93] To the degree that there is *any* formal legal authority for what is "done" on the Internet, it is possessed by INTERNIC through a series of contracts with the United States government. The *closest entity* to a governing body in cyberspace is the Internet Society (ISOC).[94] The ISOC is the voluntary membership organization that is responsible for running the Internet.[95] The mission of

---

88 An Open Letter from the World Intellectual Property Organization (WIPO) to the Internet Community Concerning Domain Name Dispute Resolution Procedures Under the gTLD-MoU. (visited June 20, 1997) <http://www.wipo.int/eng/internet/domains/openlet.htm>. The new gTLD's are: *.store* for businesses selling goods, *.firm* for businesses or firms, *.web* for organizations related to the World Wide Web, *.arts* for cultural and entertainment organizations, *.rec* for recreation/entertainment organizations, *.nom* for individual or personal sites, and *.info* for organizations providing information services. Trademark regulation may be relaxed in the *.nom* domain. For example, *McDonalds.nom* should only refer to an individual and not the international fast food frachise.

89 *Id.*

90 *Id.*

91 *Id.*

92 *Id.*

93 STOLL, *supra* note 23, at 9. *See also ACLU*, 929 F. Supp at 832 ("No single entity—academic, corporate, governmental, or non-profit—administers the Internet.").

94 Gigante, *supra* note 82, at 416 ("Since the ISOC's formation, other Internet organizations have accepted it as the over-arching Internet authority."). Some scholars question whether the ISOC and its member organizations have the legal ability to regulate the Internet. *See id.* at 420-25 (providing an excellent diagram of the relationship between the organizations and institutions that purport to regulate the Internet.).

95 STOLL, *supra* note 23, at 18.

the ISOC is to promote information exchange through Internet technology.[96] The ISOC appoints the Internet Architecture Board (IAB) to approve standards and to allocate resources.[97] The voice of the Internet Community is heard through the Internet Engineering Task Force (IETF).[98] In essence, the existing structure is a voluntary association with each member free to accept all, some, or none of the benefits of membership.[99] The IAB standards are self-policing in that if the majority adopts a new standard, the hold-outs may find that they are unable to communicate with networks outside the hold-out community.

Similar to feudal fiefdoms, each region, subregion, college, or corporation is responsible for policing its part of cyberspace.[100] Thus, "[i]n network communities, rule setting and rule enforcement are highly decentralized. Typically, the rules are made and enforced at the local area network (LAN) or 'campus network' level. The university or the corporations setting up the LAN or cluster of LANs is both the legislator and the enforcer."[101] The constituent networks of the Internet usually establish Acceptable Use Policies (AUP) that controls the traffic traversing their portions of the Internet. Generally, the rules prohibit harassment, fraudulent use of accounts, unauthorized access to systems, or unsolicited commercial advertisements.[102]

In addition to the formal AUPs, there is "netiquette"[103] (network etiquette), Frequently Asked Questions (FAQ), or informal social norms that define polite or acceptable behavior in cyberspace.[104] There are numerous "unwritten" conventions in cyberspace. For example, ALL CAPITAL LETTERS is "shouting" or ":-)" means the sender is "kidding."[105] The best description of current law making and enforcement in cyberspace is that of a voluntary association with social disapproval

---

96 *Id. See also* <http://www.isoc.org>.

97 STOLL, *supra* note 23, at 18.

98 *Id. See also* <http://www.ietf.cnri.reston.va.us>.

99 STOLL, *supra* note 23, at 18.

100 WIGGINS, *supra* note 49, at 21-22.

101 Perritt, *supra* note 36, at 352.

102 WIGGINS, *supra* note 49, at 21-22.

103 *Id.* at 22-23. "'Netiquette' is a recent neologism for 'networking etiquette'." McMurdo, *supra* note 9, at 305-318 (discussing the "rules" of netiquette). *See also* Brendan P. Kehoe, *Zen and the Art of the Internet* <http://www.itec.suny.edu/SUNY/DOC/Internet/zen.html> (a bit dated collection of the rules of netiquette along with other useful information for those homesteading on the electronic frontier); STEVEN G. JONES, ed., CYBERSOCIETY: COMPUTER-MEDIATED COMMUNICATIONS AND COMMUNITY (1995).

104 Mark A. Lemley, *Shrinkwraps in Cyberspace*, 35 JURIMETRICS J. 311, 313 (1995).

105 *Id.*; *Cybershrink*, PSYCHOLOGY TODAY, 20-21 (Nov./Dec. 1995) (describing emoticons used to substitute for visual cues and emotional inflections in cyberspace); McMurdo, *supra* note 9, at 308-309.

(flames)[106] being the common sanction.[107] The usual punishment is social ostracism.[108] Individuals who are abusive may receive polite, private messages from experienced users that explain why the behavior is unacceptable, may find that their postings are ignored, or may be asked to leave the discussion. Disconnection is the ultimate possible punishment and results in exile from cyberspace. Disconnection can be either horizontal (e.g., other networks in Internet refuse to communicate with the offending site), or vertical (e.g., local service providers disable an offending individual's access).[109] While there is some resort to civil or criminal law (these attempts appear to be sporadic, at best),[110] it appears that the *potential threat* of civil or criminal sanctions is usually sufficient when coupled with self-help or collective sanctions.[111] An example of this was cyberspace's response to the Communications Decency Act,[112] numerous World Wide Web sites with sexually oriented content have added some sort of filter from a *de minimis* java script warning the potential viewer of the nature of the websites' contents and asking the potential viewer if he or she is over 18 or is legally an adult in his or her own country. Other websites require "Adult Checks" or other proof that the viewer is legally an adult. Many of these sites are not subject to the domestic laws of the United States, yet they are striving to comply with U.S. law.

In sum, cyberspace needs no national defense and little law enforcement because each individual is charged with protecting his or her own Cyberian community. Further, existing governments have a vested interest in protecting cyberspace — or at least in protecting their citizens' economic interests in cyberspace.

Some criticisms of the current governance of cyberspace are:

---

106 Flames are "virulent and (often) personal attacks against the author of [an offending] posting." KROL, *supra* note 58, at 590. Flames have been described as "severe criticism—the digital equivalent of tarring and feathering someone on the net who has posted disagreeable material." Jason Kay, Note, *Sexuality, Live Without a Net: Regulating Obscenity and Indecency on the Global Network*, 4 S. CAL. INTERDISC. L.J. 355, 384 (1995).

107 "Very little enforcement of rules on the Internet is done by formal action taken by network authorities. Instead, peer pressure and the authority of local system administrators are the main means of enforcement." WIGGINS, *supra* note 49, at 22. *See also* Julian Dibbell, *A Rape in Cyberspace or How an Evil Clown, A Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society*, 1994 ANN. SURV. AM. L. 471, 484-85 (1994) (a detailed narrative of the events leading up to and after a "cyber-rape" on LamdaMOO); Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspace*, 104 YALE L.J. 1639, 1661 (1995).

108 Dibbell, *supra* note 107, at 480.

109 Dunne, *supra* note 1, at 12.

110 *Id.* at 7-8; Zembek, *supra* note 66, at 357-58.

111 *Cf.* Karl N. Llewellyn, *What Price Contract?: An Essay in Perspective*, 40 YALE L. J. 704, 725 n.47 (1931); Stewart Macaulay, *Elegant Models, Empirical Pictures, and the Complexities of Contract*, 11 L. & SOC'Y REV. 507, 519-20 (1977).

112 47 U.S.C. § 223 (1994).

(1) "It is too dependent on the goodwill of a small group of people who are doing the job largely by historical accident, because they were in the right place at the right time."
(2) "The most popular gTLDs are handled by an organization which holds a monopoly over registration and award of those domain names. As Adam Smith pointed out, a private monopoly is potentially worse than a public one."
(3) "The current system is dominated by actors in just one country, the United States to the exclusion of others."
(4) "It does not give adequate attention to the protection of trademarks and other intellectual property." And most importantly,
(5) "It lacks formal structure and legitimization."[113]

C. CONSTITUENT COMMUNITIES OF CYBERSPACE

Many communities collectively comprise cyberspace.[114] Cyberspace communities are known in the research literature as Computer-Supported Social Networks and are usually text based.[115] Because of the limited social presence, on-line conversations tend to be more uninhibited, creative, and blunt than face-to-face conversations.[116] To compensate for this lack of social presence, Cyberian have adopted text based signals called "emoticons" to convey cues which in other contexts are conveyed through body language. The classic example of this is the ":-)" or smiley face. The smiley face states the message should be read in a jocular or non-serious sense. As in the real world, individuals are members of different communities, and as in the real world, cyberspace communities fracture internally, develop shifting coalitions, or are hostile to outside groups.[117]

---

113 *Internet Governance: Towards Voluntary Multilateralism*, Keynote Address by Dr. Pekka Tarjanne, ITU Secretary-General (visited June 30, 1997) <http://www.itu.int/PPI/projects/dns-meet/KeynoteAddress.htm>.

114 Not all individuals use all the possible resources in cyberspace. Some individuals may only use E-mail, listserves, or the world wide web while others use Internet Relay Chat, MOOs, and other facilities that build a sense of community. Many individuals limit their access to Usenet newsgroups and exchanges information. This varying level of involvement may have an impact on who ultimately is a Cyberian. The higher the individual level(s) of social interaction and commitment to a Cyberian community, the more effectively the community can apply social sanctions. *See* Perritt, *supra* note 36, at 360.

115 Wellman, et al., *supra* note 26, at 213.

116 *Id.*

117 Perritt, *supra* note 36, at 360; Phillip Elmer-Dewitt, *Battle for the Soul of the* Internet, TIME, July 25, 1994, at 50.

Communities in cyberspace are defined largely by the technology used to communicate within cyberspace. Some communities exist largely as e-mail and may be as cohesive as a group of pen pals.[118] Other groups are highly interactive in real-time, for example the MUDS, MOOs, and talkers.[119] In these communities, individuals develop persona and exchange information in a virtual environment of their own creation.[120] Finally, some communities like the World Wide Web may be a mixture of different types of communities. For some, the World Wide Web is the old fashioned general store where people go to exchange gossip as well as goods; for others, the World Wide Web is merely a modern shopping mall or a tourist center where one goes for impersonal commerce or to see the sites. Depending on the individual's relationship to the community which is largely defined by the technology that makes the community possible, the individual may have a very simple connection to the community or a very complex relationship.

These communal loyalties affect how the individual relates to others in cyberspace. Each community has its own customs and traditions, which must be considered when developing a regulatory scheme for cyberspace. Within any of these groups, there may be a few, or in the case of Usenet, literally thousands of sub-communities, many of which have nothing in common but those similarities forced on the community by a shared technology.[121]

D. DEMOGRAPHICS OF CYBERSPACE

The problem in determining the size of the Internet is in reaching agreement on what is part of the Internet.[122] Estimates of the number of

---

118 Even communities that exist largely as e-mail, such as listserves, can be vibrant. Ongoing debates and gossip from listserves are often a staple conversation when the individuals meet in real life.

119 David Jacobson, *Contexts and Cues in Cyberspace: The Pragmatics of Naming in Text-Based Virtual Realities*, 52 J. OF ANTHROPOLOGICAL RESEARCH 461 (1996).

120 *Id.* at 463-65.

121 *Cf.* Byassee, *supra* note 7, at 198-199 ("The exact boundaries of cyberspace are indistinct, and many sub-communities have little interest or ability in communications with other parts of cyberspace."); Peter Kollock & Marc Smith, *Managing the Virtual Commons: Cooperation and Conflict in Computer Communities* (visited May 1, 1996) <http://www.sscnet.ucla.edu/soc/csoc/vcommons.htm>.

122 Quarterman & Carl-Mitchell, *supra* note 47 at 4(8). In January 1997, Matrix Information and Directory Service (MIDS) estimated that there were "36 million users of computers that can *distribute* information by interactive TCP/IP services such as WWW of FTP ('core Internet')," "57 million users of computers that can access information by interactive TCP/IP services ("consumer Internet")," and "71 million users of electronic mail ("the matrix")." Quarterman, *supra* note 8, at 1. Future projections for Internet growth for the year 2001 are 827 million Matrix users, 707 million Consumer Internet users, 436 Core Internet users, and 254 million Internet hosts with IP addresses. *Id.*

users have ranged between three million and sixty million.[123] But, conventional wisdom dictates that cyberspace has been increasing at the monthly rate of 15 percent, and currently, there are approximately 2.2 million computers and over twenty million users in 135 countries.[124] These numbers are expected to grow for the foreseeable future.[125]

Nielsen Media Research (NMR) estimated that 37 million people in the United States and Canada have access to the Internet either directly, through a commercial ISP, or through a friend, and that 17 percent of the population aged sixteen and older (24 million people) had, in the prior 3 months, spent an average of 5.5 hours per week on the Internet.[126] NMR also estimated that 34 percent of the users are women, 66 percent accessed the Internet from work, and 25 percent of the World Wide Web users had incomes in excess of $80,000. These statistics suggest a large and relatively affluent Internet population.

E. REVENUE

Historically, the Internet was largely supported by government and academic institutions who bore the infrastructure and administrative costs.[127] Current usage patterns, particularly for individuals with Internet access through a college or university, give the illusion that the Internet is "free."[128] But there are no free riders in cyberspace. Although no one pays for cyberspace, each network supports its part.[129] "The NSF paid for NSFNET. NASA pays for the NASA Science Internet. A college or corporation pays for its connection to a regional network, which in turn pays a national provider for its access."[130] Depending on the institution's function, the institution's traffic may be routed on either not-for-profit or commercial routes. Research and educational institutions gener-

---

123 Julian Dibbell, *Nielsen Rates the Net the Folks Who Measure TV Usage Produce the First Solid Survey of the Internet. Their Finding: It's Nearly ready for Prime Time*, TIME, Nov. 13, 1995, at 121; Keith A. Ditthavong, *Paving the Way for Women on the Information Superhighway: Curbing Sexism Not Freedoms*, 4 AM. U. J. GENDER & L. 455, 510 n.38 (1996) (discussing studies of Internet usage).

124 Ryga, *supra* note 7, at 223. As of July 1996, there were at least thirty-three nations completely unconnected to the Internet. Wu, *supra* note 27, at 651.

125 Ryga, *supra* note 7, at 223.

126 Dibbell, *supra* note 123, at 121 (based on a telephone survey of 4,200 households in the United States and Canada). Nielsen Media Research's methodology has been severely criticized. Rajiv M. Rao, *Nielsen's Internet Survey: Does it Carry any Weight?*, FORTUNE, Mar. 18, 1996, at 24. Critics claim that "the numbers are bunk" and allege that the survey answers were weighted incorrectly to compensate for sampling errors. *Id.*

127 Lori Hawkins, *Increased Net Surcharge Suggested: UT Researchers Say Higher Fees at Peak Hours Might Ease Logjams*, AUSTIN AMERICAN-STATESMAN, Nov. 7, 1996, at C1.

128 *See* DEPARTMENT OF DEFENSE, THE NEXT GENERATION INTERNET: ANOTHER STEP IN THE SUCCESSFUL TRANSITION TO THE COMMERCIAL INTERNET (1996).

129 Dunne, *supra* note 1, at 19.

130 *Id.*

ally use the National Research and Education Network (NREN).[131] Commercial organizations generally contract with commercial Internet providers.[132] Many institutions treat Internet access as an annual fixed cost so that users are not charged based on volume.[133] Commercial providers account for the costs in setting access charges, and some providers control costs by rationing the quantity or types of services.[134] The NSF is progressing from a government supported Internet to a commercial Internet.[135] Because everyone must enter cyberspace through an Internet Service Provider, tolls can easily be imposed at the "on-ramp."[136] Currently, there is some discussion of manipulating net usage through pricing strategies to conserve infrastructure resources.[137] Unlike traditional jurisdictions, which must raise revenue through taxes in order to support building a national infrastructure or pay for essential services, all expenses in cyberspace are paid through user fees. The high speed communications networks will be provided because the telecommunications industry will find it profitable to charge users fees for access to the network. Cyberspace, like self-supporting communal communities, devolves power to the lowest levels where that power will be effectively utilized out of enlightened self-interest. Accordingly, the financing of cyberspace is remarkably efficient and occurs without the coercive power of the state exacting taxes or transferring wealth.[138]

---

131 KROL, *supra* note 58, at 596. NREN is an attempt of the United States government to combine the separate federal agency networks into a single high-speed network.

132 *Id.* For example, some of the major commercial providers are: Advanced Networks, Services (ANS), Performance Systems International (PSI), and UUNET. In addition, there are state and regional providers. These services are interconnected and interoperate legally by using creative accounting agreements to allocate costs. *Id.* For a general discussion of the "political economy" of cyberspace, see Jeffrey K. Mackle-Mason & Hal R. Varian, *Economic FAQs about The Internet* (visited 5/20/97) <http://www.ipps.lsa.umich.edu/ipps/papers/infonets/Economic_FAQs/FAQs/FAQs.html>.

133 WIGGINS, *supra* note 49, at 21.

134 *Id.*

135 DEPARTMENT OF DEFENSE, *supra* note 76, at 1.

136 If the reader examines Figure 1, he or she will note that it is impossible to enter cyberspace except through an ISP.

137 *See* Hawkins, *supra* note 127, at C1 (Internet users may have to pay during peak hours to prevent traffic jams.).

138 Some day, Cyberians may be faced with choosing between increasing user fees to support universal access or tolerating a significant problem of free-riders. *Cf.* Werbach, *supra* note 48, at 35 & nn.76-78 (quoting Federal-State Joint Board on Universal Service, Recommended Decision, FCC 96J-3, CC Docket No. 96-45, at 398 ¶¶790-91) (The FCC convened a federal-state joint board to recommend a funding source for universal service. The joint board recommended that information and enhanced service providers do not have to contribute to the universal service funding mechanism; but, ISPs that provide services to schools and libraries are eligible for universal service subsidies.); *see* 47 U.S.C. § 254 (1994) (providing that all interstate telecommunications carriers must contribute to universal service). This obviously raises questions of equity.

III. REGULATION, SELF-REGULATION, OR NO REGULATION

The regulation of cyberspace may take one of three forms. Cyberia will be government regulated, self-regulated, or even unregulated. The choice is not between an idyllic state of no regulation, self-regulation, and government regulation, but which mixture of the three. This regulation may be an addition to existing legal structures. Already, the virtual denizens of cyberspace are subject to laws governing their physical domicile — virtual crimes, torts, and breaches of contract can be punished or remedied by the "real" courts of a temporal sovereign.[139] Additionally, Cyberians are governed by the existing formal and informal social norms of cyberspace and the rules of their ISPs.

If government regulation is to be the primary means of governing cyberspace then are existing laws for "real space" harmonious in cyberspace, or does cyberspace require a new regime of laws that are drafted especially for the unique social, economic, political, and technical environment that constitutes cyberspace?[140] Initially, a *sui generis* law of cyberspace is attractive, but the denizens of cyberspace are already subject to international, transnational, national, and local laws. As a general rule, when the level of statutory and regulatory complexity rises, so do transaction costs, while the certainty that any given Cyberian act is legal decreases.[141] A *sui generis* law of cyberspace merely adds one more level of complexity to the law and more confusion to an already unnecessarily complex legal system.[142]

The unstated assumption is that the model that solves the problem with the fewest externalities and costs is the best — or, to paraphrase Thoreau, the government that governs the least governs the best.[143] Two rules should be considered when evaluating the propriety of new laws for cyberspace. A first general rule is to examine existing law and determine

---

139 *See, e.g.*, William S. Byassee, *supra* note 7, at 199; DAVID ICOVE ET AL., COMPUTER CRIME: A CRIMEFIGHTER'S HANDBOOK 205-349 (1996) (reprinting major federal, state, and foreign computer crime laws); Zembek, *supra* note 66, at 346-47.

140 I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U. PITT. L. REV. 993, 995 (1994).

141 Legal uncertainty is reflected in the market price of access, content, and goods sold in cyberspace. Because everyone in cyberspace is potentially both a publisher and consumer of content, individuals who provide content at low or no-cost may decide not to provide content until the legal status of the content or transaction is established. This phenomenon is clearly demonstrated by the chill which the Communications Decency Act of 1996 places on information transactions in cyberspace. *See, e.g.*, ACLU v. Reno, 929 F. Supp. 830, 877-78 (E.D. Pa. 1996) (Dalzell, J., supporting opinion), *aff'd* 1997 WL 348012 (1997).

142 Unless the new *sui generis* regime of laws displaces or preempts existing law for the "real world." *Cf.* Nimmer, *supra* note 5, at ¶ 1.102[4].

143 "I heartily accept the motto, 'That government is best which governs least'; and I should like to see it acted up to more rapidly and systematically. Carried out, it finally amounts to this, which also I believe, 'That government is best which governs not at all.'" HENRY DAVID THOREAU, CIVIL DISOBEDIENCE 1 (1849).

whether it fits into the paradigm of cyberspace. Also, examine whether the purposes and policies behind the existing law efficiently effectuate the same purposes and policies in cyberspace.[144] A second general rule is to balance the costs and benefits of enacting special legislation for cyberspace.[145] Therefore, if existing ambiguous legal relations do not impose significant costs on routine behavior, then a special law of cyberspace is not justified. However, if the ambiguous legal relationship imposes significant costs on routine behavior, then a special law of cyberspace may be justified.[146] Because existing law either literally, by analogy, or by metaphor applies to cyberspace, rarely will *sui generis* laws for cyberspace be justified.

The criticism of the law and economics approach is that it is value neutral.[147] In cyberspace, this is also the approach's strength. "Thirty-seven million users in 161 countries connect to each other generating 100 million e-mail messages every day."[148] Each of those 161 countries has its own domestic laws, customs, religious beliefs, and morality. Within these countries, there are numerous subcultures, each with distinct variations on the national culture. Sometimes these subcultures exist in apposition or opposition to the dominant culture. To impose a culture on cyberspace would be to balkanize it.[149] The law and economics approach has the advantage of respecting individual differences, thus resolving values and moral issues in the marketplace of cyberspace.[150] Each ideology, value, code of conduct, or custom may compete freely for acceptance in the marketplace. Some values will fall by the wayside, others will be assimilated, and still others will remain in active competition to become the dominant paradigm.

---

144 Hardy, *supra* note 140, at 996; David R. Johnson & Kevin A. Marks, *Mapping Electronic Data Communications onto Our Existing Legal Metaphors: Should We Let Our Conscience (and Our Contracts) Be Our Guide?*, 38 VILL. L. REV. 487, 515 (1993).

145 Hardy, *supra* note 140, at 998.

146 *Id.* The costs do not have to be economic costs. *Cf.* Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833, 843 (1992)("Liberty finds no refuge in a jurisprudence of doubt.").

147 *See generally* Jane B. Baron & Jeffrey L. Dunoff, *Against Market Rationality: Moral Critiques of Economic Analysis in Legal Theory*, 17 CARDOZO L. REV. 431 (1996); Lawrence M. Friedman, *Two Faces of Law*, 1984 WIS. L. REV. 13, 15-16 (1984). Admittedly, this position is not neutral to the proposition that competition and free markets solve most problems, but every theory must have at least one axiom.

148 Cate, *supra* note 14, at 565.

149 *Cf.* Lemley, *supra* note 104, at 321.

150 In a community that is defined solely by its communications media and ease of communication, transaction costs may be so marginal as to render the "law" irrelevant. *See* Lewis A. Kornhauser, *Are There Cracks in the Foundations of Spontaneous Order? Order Without Law: How Neighbors Settle Disputes*, 67 N.Y.U. L. REV. 647 (1992) ("Economic analysts of law have argued that law is important only when 'transaction costs' are sufficiently high.").

IV. NO REGULATION

The no regulation model is a null choice because, in cyberspace, the idyllic state of nature never actually existed.[151] Cyberspace is an accidental byproduct of United States government research.[152] Consequently, the United States government has always placed some regulation on cyberspace.[153] For example, the NSFNET Backbone Services Acceptable Use Policy prohibits the commercial use of NSFNET.[154] At all times the physical bodies of Cyberians could be punished for their cyberspace activities should some "real" government choose to exercise such control.[155] Yet, governments rarely attempted to extend their jurisdiction into cyberspace. But this policy of benign neglect has changed. Governments are now interested because many individuals who are currently using the Internet can afford to invoke the judicial system to resolve disputes. The popularization of the information superhighway has educated both judges and legislatures that this is a place where real wrongs take place — wrongs that are worthy of a remedy.[156] Besides government regulation, cyberspace has always had self-imposed regulations. Because cyberspace has always been regulated, this fact leads inevitably to the question of whether a *sui generis* law of cyberspace is needed or even wise.

V. GOVERNMENT REGULATION

Already, nations are aggressively attempting to regulate cyberspace.[157] This regulation takes two forms: enforcing laws of general applicability in cyberspace and creating new laws to govern cyberspace. The legal enforcement model uses positive law enforced through administrative agencies and the courts.[158] There is very little to be said for this approach. The futility of a nation-state approach to law, jurisdiction, and dispute resolution is best shown by some cyberspace aphorisms — for

---

151 *See generally* LANCE ROSE, NETLAW: YOUR RIGHTS IN THE ONLINE WORLD, xvi (1995).

152 *See supra* Part II.B.

153 The United States government has at least regulated those portions of cyberspace that it financially supported. But many, if not all, of the original settlers first explored cyberspace from a college, university, or research institution, so they were governed by these rules.

154 *See* KROL, *supra* note 58, at 575.

155 *See id.*

156 ROSE, *supra* note 151, at xvi.

157 *In the News: Governments Move to Control the Free Flow of Information on the Net*, 1 CYBERSPACE L. 27-29 (1996) (discussing the Peoples Republic of China. France, Germany, Saudi Arabia, Singapore, the United States, Vietnam, and the European Commission); *See also Human Rights Watch Report, Silencing the Net: The Threat to Freedom of Expression On-Line*, HUMAN RIGHTS WATCH, May 1996 Vol; 8, No. 2 (visited April 26, 1997) <http://www.netfreedom.org.au/anoid/nfhwr.html>.

158 Perritt, *supra* note 36, at 355.

example, "In cyberspace, the First Amendment is merely a local ordinance"[159] or "National borders are mere speed bumps in cyberspace."[160] In cyberspace, distance is measured in nanoseconds[161] — not miles. Social interaction or commercial transactions on a transnational level are possible with an ease heretofore only imagined by science fiction writers who dreamed of teleportation devices.[162] Accordingly, one is as likely to have an international dispute as a national one. The function of dynamic routing and facilities such as the World Wide Web, File Transfer Protocol, and remote log-on/telnet permit a user to enter, or at least to cross numerous national, state, or local borders without either the user or national authorities being aware of the user's passage.[163] Therefore, "[t]raditional notions of jurisdiction are outdated in a world divided not into nations, states, and provinces but networks, domains, and hosts."[164] Trying to regulate cyberspace on a country-by-country basis is doomed to fail because it is inefficient and does not account for the inherent nature of the technology.[165] "The Internet is wholly insenstive to geographic distinctions. In almost every case, users of the Internet neither know nor care about the physical location of the Internet resources they access. Internet protocols were designed to ignore rather than document geographic location."[166] "[T]he unique nature of cyberspace necessitates uniform national treatment and bars the states from enacting inconsistent regulatory schemes."[167] Similary, the unique nature of the cyberspace requires a uniform global system of regulation should bar nation-states from enacting inconsistent national legislation.

---

159 John Perry Barlow <http://www.lexmark.com/data/alpha-b.html>.

160 Timothy C. May <http://boojie.rt.csuohio.edu/~31337/cun/cun07-16-96>.

161 A nanosecond is one billionth of a second (10^{-9}). THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE, *supra* note 15, at 1200.

162 *See, e.g.*, CompuServe, Inc. v. Patterson, 89 F.3d 1257, 1262 (6th Cir. 1996); Dept of the Treasury, *Selected Tax Policy Implications of Global Electronic Commerce* (visited April 25, 1997) <http://www.ustreas.gov/treasury/internet.html> ("These new technologies, particularly communications technologies including the Internet, have effectively eliminated national borders on the Information highway.").

163 Matthew R. Burnstein, Note, *Conflicts On the Net: Choice of Law in Transnational Cyberspace*, 29 VAND. J. TRANSNAT'L L. 75, 81-82 (1996). "For example, hypertext on the World Wide Web enables users to 'visit' one location (called a page or site), where they are then presented with an opportunity to visit any of a number of other locations—in any of a number of other countries." *Id.* at 82.

164 *Id.* at 81. *But see* Zembek, *supra* note 66, at 367.

165 *Cf.* American Library Ass'n v. Pataki, 97-Civ.-0222(LAP) (S.D.N.Y.) (visited July 1, 1997) <http://chronicle.com/che-data/focus.dir/data.dir/0623.97/ala.htm> (holding that the unique nature of the Internet prohibited state regulation under the Commerce Clause).

166 *Id.*

167 *Id.*

A. THE COMMUNICATIONS DECENCY ACT: COLONIALISM IN CYBERSPACE?

Most attempts to regulate cyberspace have been imposed from without. Governments so far have not attempted to work within Cyberian structures to build a consensus for their policies nor have they attempted to work through Cyberian elites. This creates the perception that *outsiders*[168] are attempting to regulate cyberspace which Cyberians reject as illegitimate "[i]t is, . . . as though 'the illiterate could tell you what to read.'"[169] This disconnect between the governors and the governed quickly lead to analogies between the colonial powers and indigenous people, and ultimately, "A Declaration of Independence of Cyberspace."[170] As John Perry Barlow stated in *A Declaration of Independence of Cyberspace*

> Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. . . . You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society with more order that could be obtained by any of your impositions.[171]

The CDA was not the first attempt by government to regulate cyberspace[172], but it was the attempt that defined Cyberia as a community-in-opposition. The United States pioneered the Internet and plays an important role in the future development of the Internet.[173] Other countries may model their domestic and international cyberspace policy on the United States expecting that the United States "as the inventor of the Internet and the world's foremost technological superpower [should] take the lead in creating the policy framework for the new world."[174] The Cyberian community rejected the Communications Decency Act because

---

168 For example, the Communications Decency Act's sponsor in the United States Senate, Senator J. J. Exon, never entered cyberspace until shortly before defending the CDA on the Senate floor. *See* Paul Goodsell, *Exon Went On-Line Before Vote Experience Helped In Debate on Porn*, OMAHA WORLD-HERALD, June 16, 1995, at 2. Bob Peters of Morality in Media admitted that he had never been on the Internet and had declined numerous offers for a tour of cyberspace. *See* Robert Peters, Remarks at 1996 *Cornell Journal of Law and Public Policy* Symposium: Regulating Cyberspace: Is Censorship Sensible? (Apr. 13, 1996).

169 John Perry Barlow <http://132.74.18.2/~dkalekin/declar1.txt>.

170 *Id.*

171 *Id.*

172 *See* notes 28, 157 & 187.

173 Burton, *supra* note 2 at 30.

174 *Id.* at 31. The United States accounts for approximately two-thirds of the world's Internet users and hosts. *Id.* at 32.

it was a paradigm for illegitimate government regulation in cyberspace. Accordingly, Cyberians chose the CDA as the issue on which to take a stand.

A premise of democracy is legislation without representation is tyranny. The Cyberian community is large and politically aware. There are numerous lobbying and interest groups that represent Cyberians or at least have a colorable claim of representing some segment of the community.[175] Yet the United States Congress passed the Communications Decency Act without hearings.[176] So the voice of the Internet community was not heard.[177] Prior to passage, the Clinton administration expressed its view to Congress that the CDA was unnecessary because "existing laws already authorized its ongoing efforts to prosecute obscenity, child pornography, and child solicitation."[178] Finally, the law as passed was unconstitutional. Attorney General Janet Reno wrote a letter to House Speaker Newt Gingrich that the United States Department of Justice considered those portions of the CDA that prohibited the interstate transmission of communications on the topic of abortion was a violation of the First Amendment.[179] Thus the CDA was an unnecessary sui generis law for cyberspace passed without hearing from the Cyberian constituency, developing a record that the CDA was appropriate for the unique conditions of cyberspace, and added unnecessary complexity and ambiguity to legal relations in cyberspace without any corresponding benefits. In sum, the CDA is the model of what this article contends that legislatures should not do in cyberspace.[180]

---

175 For example, the American Civil Liberties Union, Human Rights Watch, Electronic Privacy Information Center, Electronic Frontier Foundation, Computer Professionals for Social Responsibility, America Online, CompuServe, Netcom, Prodigy, Internet Society, etc.

176 *See* S. Rep. No. 104-23 9 (1995); *Cyberporn and Children: The Scope of the Problem, The State of the Technology, and the Need for Congressional Action, Hearing on S. 892 before the Senate Committee on the Judiciary*, 104th Cong. 7-8 (1995).

177 This presupposes the voice of Cyberians in the United States would be adequate to represent a global community.

178 ACLU, 1997 WL 348012 *17 (citing 141 Cong. Rec. S8342 (June 14, 1995) (letter from Kent Marcus, Acting Assistant Attorney General, U.S. Dep't of Justice to Sen. Leahy). Tellingly, after the CDA was declared unconstitutional, the Clinton Administration changed its Internet policy again. Jeffrey R. Young, *New White House Internet Policy Avoids Regulation of Content*, CHRON. HIGHER ED. A20 (July 11, 1997). The new policy called for a "system of content ratings and filtering technology" consistent with the First Amendment. *Id.*

179 142 Cong. Rec. S1598-03, *S1599 (Letter from Janet Reno, Attorney General to Newt Gingrich); ACLU v. Reno, 929 F. Supp. 824, 829 (1996) ("the Department has a longstanding policy that [limitations on the discussion of abortion] are unconstitutional and will not be enforced", and that both President Clinton and Attorney General Reno "have made th[e] point clear" that no one will be prosecuted under "the abortion-related provision").

180 Shortly before this article went to press, the United States Supreme Court in *Reno v. ACLU* declared the challenged portions of the CDA unconstitutional. 1997 WL 348012, *10 (affirming the district court's injunction against the government enforcing 47 U.S.C.A. § 223(d)(1)-(2) and § 223(a)(1)(B) (West Supp. 1997) insofar as it relates to "indecent" communication). Further the Clinton Administration stated that it "supports industry self-regula-

B. TRADITIONAL CHOICE OF LAW REGIME

Rather than create a *sui generis* law for cyberspace, nations may decide to treat cyberspace as a special type of transnational transaction and subject any dispute arising from the transaction to traditional choice of law analysis (in order to decide whose law and which forum will adjudicate the dispute). Countries could apply either the law of the place of the wrong or the law of the place with the most significant relationship to the transaction.[181] In cyberspace (because of dynamic routing and the conceptual difficulties of applying a land based geographic metaphor), when applying the law of the place of the wrong to cyberspace, the "place of the wrong" will often be indeterminable or at least hotly contested. If the place of the wrong cannot be determined, the tribunal will most likely apply to law of the forum adjudicating the dispute.[182]

The second option is to apply the law of the jurisdiction with the most significant relationship to the dispute. This approach is also problematic. Section 145 of the Restatement (Second) of the Conflict of Laws applies a nebulous seven-factor balancing test.[183] Section 145 requires courts to consider:

(1) the needs of interstate and international system;
(2) the policies of the forum;
(3) the policies of other interested states;
(4) the expectations of the parties;
(5) the core policies underlying the law;
(6) the certainty and uniformity of result; and
(7) the ease of determining and applying the law.[184]

These factors are not easily balanced in cyberspace.[185] Therefore, there is no simple and fair test to anticipate which jurisdiction's laws will govern a particular transaction. For example, the moment the tort is committed, every country on the Internet has at least a tangential connection to the tort because of their connection to cyberspace.

---

tion, adoption of competing ratings systems, and the development of easy-to-use technical solutions." *A Framework for Global Electronic Commerce* (visited July 2, 1997) <http://wwww.whitehouse.gov/WH/Commerce/read.htm>.

181 Burnstein, *supra* note 163, at 93-94.

182 *Id.*

183 *Id.*

184 RESTATEMENT (SECOND) OF THE CONFLICT OF LAWS § 145 (1971).

185 The author leaves it to the reader's imagination about the possible permutations using the World Wide Web. The paradigm could be this simple. User in country A accesses Web page in Country B that is linked to Site in Country C. Now, assume a content on Site is illegal in country A. What are the interests of countries B & C? What are the interests of Web page and Site?

C. CYBERALTY (ADMIRALTY AND MARINE LAW)

Over centuries, laws have developed to govern one truly transnational space, the open sea. Traditionally, nations do not claim sovereignty over the sea in excess of their costal waters.[186] Similarly, nations may be willing to forego claiming sovereignty in the transnational nature of cyberspace. Admiralty and Maritime laws originated because many maritime transactions threatened to escape regulation because they were not linked to physical places within national law systems.[187] Similarly, transactions in cyberspace are escaping regulation because they have little connection to national law systems. As a general principle of maritime law, the law of the nation where the vessel is registered governs the vessel while it is in international waters.[188]

> The most important principle to recognize is that 'the general maritime law is not the law of any particular country but is part of the law of nations.' The analogy is clear: cyberspace, like the high seas calls for a unified, common understanding of the law to be chosen to adjudicate disputes.[189]

Under maritime law, the law follows the flag. By analogy in cyberspace, the law could follow the ISP. The law governing any particular transaction would be the law of the jurisdiction where the individual entered cyberspace.[190] This would be the applicable law notwithstanding the nationality of the individual.[191] By attributing the sovereignty of the ISP to the individual user, this model avoids the difficulty of *rlogin* or *telnet*,[192] which renders the geographical location of the user irrelevant.

---

186 *See, e.g.*, Convention on the Territorial Sea and the Contiguous Zone, Apr. 19, 1958, 15 U.S.T. 1606, T.I.A.S. No. 5639, 516 U.N.T.S. 205; U.N. Convention on the Law of the Sea, Oct. 7, 1982, 21 I.L.M. 1261.

187 *See generally* Perritt, *supra* note 36.

188 Geneva Convention on the High Seas, Apr. 29, 1958, 13 U.S.T. 2312, T.I.A.S. No. 5200, 450 U.N.T.S. 82; THOMAS J. SCHOENBAUM, ADMIRALTY AND MARITIME LAW § 1-12 (2d ed. 1994).

189 Burnstein, *supra* 163, at 104.

190 *Cf.* Jane C. Ginsberg, *Global Use/Territorial Rights: Private International Law Questions of the Global Information Infrastructure*, 42 J. COPYRIGHT SOC'Y U.S.A. 318, 322 n.11 (1995); *A Framework for Global Electronic Commerce* (visited July 2, 1997) <http://wwww.whitehouse.gov/WH/Commerce/read.htm> ("The rules of the 'country of origin' should serve as the basis for controlling Internet advertising to alleviate national legislative roadblocks and trade barriers.").

191 *See id.* (citing Lauritzen v. Larsen, 345 U.S. 571 (1953)) ("The nationality of the vessel for jurisdictional purposes was attributed to all her crew.").

192 *Rlogin* or *telnet* permits users to access and use computers from remote locations. For example, the author frequently accesses his computer account in Massachusetts from Florida. Under this model, if the author accessed cyberspace from his Florida account, then Florida has jurisdiction. If the author telnets to Massachusetts and accesses cyberspace from that account,

Unfortunately, this approach still does not resolve conflicts among users entering cyberspace from ISPs licensed in different countries or ISPs flying flags of convenience.[193] If there is a dispute between individuals accessing cyberspace through different national ISPs, this dispute must be resolved through some choice of law paradigm. But, existing choice of law rules do not fit neatly into cyberspace. Further, this could create a race to the bottom. Countries that are information poor or which do not produce substantial intellectual property could become flags of convenience for ISPs. These countries could refuse to recognize intellectual property or property interests in one's reputation.[194] Sophisticated users could then *rlogin* or *telnet* into a data haven and then hoist the "Jolly Roger" and engage in intellectual or reputational property piracy with little danger of being punished in his or her geographical place of domicile. Nations may decide to pierce the ISP veil to insure that their domicillairies are complying with the local national law. While the tradition of the law of the sea clearly demonstrates that nations can yield sovereign authority in transnational space, this process has taken centuries and a complex regime of at least 63 different treaties (in addition to tradition and custom) that in some way address rights, duties, or privileges involving maritime law.[195]

D. A CONVENTION ON THE LAW OF CYBERSPACE: THE INTERNATIONAL TELECOMMUNICATIONS UNION

The International Telecommunications Union is a specialized agency of the United Nations that is responsible for the regulation of international telecommunications.[196] This existing structure could foreshadow international regulation of cyberspace. Already, the ITU cosponsored a conference to resolve a major dispute over generic top-level domain names, and in doing so, internationalized a process that once was solely a United States domestic matter. Morever, there are numerous multinational conventions that govern international transactions.[197] Nonetheless, it is unlikely that individual countries will surrender that

---

then Massachusetts has jurisdiction even though the author was physically in Florida at the time.

193 Nor does it guarantee that there will be a person there to exercise jurisdiction over.

194 *See* Dan L. Burke, *Patents in Cyberspace*, 68 TUL. L. REV. 1, 13 (1993) (noting that some nations have no patent law at all).

195 LOUIS B. SOHN & KRISTEN GUSTAFSON, THE LAW OF THE SEA IN A NUTSHELL, at xxiii-xxxvi (1984) (listing treaties, conventions, and agreements between 1883 and 1980).

196 *See* White & Lauria, *supra* note 4, at 2.

197 *See* Burnstein, *supra* note 163, at 113 & nn.234-243. For Cyberians, international agreements that eventually govern other frontiers: outer space, the moon, or Antarctica (i.e., "regions within the reach and use of nations but not easily demarcated into jurisdictions") may foreshadow the future law of cyberspace. Conversely, nations may use the law of inner-space (cyberspace) as a model for closing the remaining frontiers.

degree of sovereignty over individuals who are physically present within the geographical boundaries of the country that is necessary to create a public law of cyberspace. Secretary-General Pekka Tarjanne of the ITU stated that the

> central strategic challenges' facing the ITU today is the need to adopt the 'principles and presuppositions of national sovereignty and multilateralism . . .' to the realities of a telecommunication industry which is creating the global information society of the future.[198]

A pragmatic option is a treaty that establishes a private law of cyberspace.[199] Such a treaty could formally recognize the right of Cyberians to engage in private law making and private ordering of their own affairs. Nations already allow for the private ordering of international commercial transactions. The Convention on the International Sales of Goods (CISG)[200] permits parties to enter into enforceable contracts for the sale of goods, and the United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards (the New York Convention)[201] permits parties to create their own private courts to enforce private laws. Under a treaty, nations could formally grant broad authority to individuals in cyberspace and create an international body to study the effects and make suggestions for improving the treaty over-time. Already, the United Nations Commission on International Trade Law (UNCITRAL) has drafted a model law that encourages the used of international contracts to facilitate electronic commerce.[202] Because cyberspace is the modern equivalent to the traditional marketplace or agora in that it is a marketplace of intellectual property, goods, services, and "speech," the Convention should enshrine fundamental principles of human rights that may not be waived.[203]

---

198 White & Lauria, *supra* note 4, at 30 (quoting Pekka Tarjanne, *The ITU Responds to New Concepts for Public Policy in the Global Information Society*, 20 INTERMEDIA 6, 13 (1992)).

199 The United States and the European Union would support a private law of cyberspace, at least in principle. *See A Framework for Global Electronic Commerce* (vistited July 2, 1997) <http://wwww.whitehouse.gov/WH/Commerce/read.htm>; *EU Council of Ministers Conclusions: 12102/96*, THE REUTER EUROPEAN COMMUNITY REPORT (Nov. 29, 1996).

200 U.N. CONVENTION ON CONTRACTS FOR THE INTERNATIONAL SALE OF GOODS, FINAL ACT, U.N. Doc. A/CONF.97/18 (1980).

201 Convention on the Recognition and Enforcement of Foreign Arbitral Awards, June 10, 1958, 21 U.S.T. 2517, T.I.A.S. No. 6997, 330 U.N.T.S. 3, *reprinted in* 9 U.S.C.A. §§ 201-208 (West 1992).

202 *A Framework for Global Electronic Commerce* (vistited July 2, 1997) <http://wwww.whitehouse.gov/WH/Commerce/read.htm>.

203 In keeping with the political traditions of the United States that civil rights are protections from government (and not one's fellow citizens), the Clinton Admistration's "A Framework for Global Electronic Commerce" seeks to open a dialogue to ensure that national regulation does not serve as disguised trade barriers. In cyberspace, speech may need protec-

VI. NON-GOVERNMENT REGULATION OF CYBERSPACE

Self-government or self-regulation is usually justified if it is: (1) more efficient; (2) the rules or adjudicatory procedures differ from the surrounding community; (3) the rules of the surrounding community are inapplicable; or (4) compliance with the rules of the community is higher, if the rules are self-enforced.[204] Although all four factors support a self-regulation, this section will focus on the first. The jurisdictional and sovereignty issues in cyberspace makes it difficult for territory based nation states to enforce their laws on cyberspace. Even if jurisdictional issues are solved, the infrastructure of cyberspace is evolving too rapidly for governments to regulate efficiently.[205] The unique technical and transnational nature of cyberspace justifies self-government. The aphorism that technology leads and the law follows best expresses this point. "It cannot be helped, it is as it should be, that the law is behind the times."[206] In 1915, the United States Supreme Court held that motion pictures were "spectacles, not to be regarded . . . as part of the press of the country or as organs of public opinion."[207] And again, in 1968, a federal court held that "the public has about as much real need for the services of a CATV system as it does for hand-carved ivy back-scratchers."[208] "Prosecutors and judges generally are not familiar with the culture and norms of the Internet. They may lack the technical expertise necessary to identify and prosecute offenders."[209] Overall, the legislatures, regulatory agencies, and courts do not appear to be percipient in

---

tion from both government and citizenry. Nelson Mandela observed that "In the 21st century, the right to communicate will be the main human right." Sean Selin, Comment *Governing Cyberspace: the Need for an International Solution*, 32 GONZ. L. REV. 365, 365 (1996-97)(citation omitted).

204 Perritt, *supra* note 29, at 31; see also Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARV. J.L. & TECH. 465, 477-490 (1997).

205 SOLA POOL, TECHNOLOGIES OF FREEDOM 7 (1983) (recognizing the essential challenges of analogizing new technology to existing law); LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW 1007 (2d ed. 1988) ("The rate of technological change has outstripped the ability of the law, lurching from one precedent to another, to address new realities."). Both the United States, A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE (visited July 2, 1997) <http://wwww.whitehouse.gov/WH/Commerce/read.htm>, and the *Council of Minsters of the European Union, Conclusions of the Nov. 28 Telecommunications Council*, THE REUTERS EUROPEAN COMMUNITY REPORT (Nov. 29, 1996), have expressed strong support for self-regulation and encouraging private sector initiatives to develop procedures and policies that facilitate operation of cyberspace.

206 SPEECHES OF OLIVER WENDELL HOLMES 102 (1934) *quoted in* NIMMER, *supra* note 5, at § 1.02.

207 Mutual Film Corp. v. Indus. Comm'n of Ohio, 236 U.S. 230, 244 (1915), *overruled by* Joseph Burstyn Inc. v. Wilson, 343 U.S. 495 (1952).

208 Greater Fremont, Inc. v. Fremont, 302 F. Supp. 652, 663 (N.D. Ohio 1968), *aff'd sub nom* Wonderland Ventures, Inc. v. Sandusky, 423 F.2d 548 (6th Cir. 1970).

209 Lemley, *supra* note 104, at 314.

anticipating the economic and social impact of new technology.[210] This lack of foresight suggests that these institutions should not *unnecessarily* exercise their existing authority and not seek new authority to regulate cyberspace until either the technology and its implications become predictable or the institutions and customs of cyberspace have an opportunity to develop in response to the needs of Cyberian constituent communities and commerce. Accordingly, governments should encourage a self-regulation model.

A. SELF-HELP AND SOCIAL ENFORCEMENT MODELS

Two basic models of community regulation are a self-help model and a social enforcement model.[211] As in the "real world," self-help and the social enforcement models are the core basis on which an efficient ordering of cyberspace will be based. The self-help model allows the individual to exit from situations in cyberspace that the individual finds inappropriate. The social enforcement model allows individuals to form communities in cyberspace that express their individual values and expectations and to exclude others who to do share those values or who are unprepared or unwilling to comply with community norms.[212]

This article will consider each in turn and compare forms of rulemaking that are least restrictive, most decentralized, and cost effective to those that are more centralized, restrictive, and cost inefficient. Through this process, the article emerges at the third model — private law, self-regulation, through a contract law paradigm which is best suited to govern cyberspace. The contract law model is most frequently offered as the governing paradigm for cyberspace.[213] Contract law has much to commend it. Contracts as a source of legitimacy and justification, for governance has a long and honorable lineage.[214] Contract at its best is the expression of the free will of individuals freely acting to maximize their personal welfare.[215]

1. *Unilateral Avoidance: The Self-Help Model*

Probably, the simplest model of rule making, the most effective, and the most cost-efficient is the self-enforcing one. The model is self-help (i.e., "you don't like it, don't do it or stop people from doing it to

---

210 *See* Gordon & McKenzie, *supra* note 17, at 194-95.

211 *See* Perritt, *supra* note 36, at 354.

212 Perritt, *supra* note 25, at 1017-19 & n. 55 (citing GEORGE D. WEBSTER, THE LAW OF ASSOCIATIONS § 2.03(1) (b) (1993)). Both models suffer from one major defect, however, neither controls individuals who are not part of the community.

213 *See, e.g.*, Burnstein, *supra* note 163, at 97; Dunne, *supra* note 1, at 11-15; Johnson & Marks, *supra* note 90, at 488-89; Perritt, *supra* note 36, at 355.

214 *See generally* Rosenfeld, *supra* note 33.

215 Alex Y. Seita, *Uncertainty and Contract Law*, 46 U. PITT. L. REV. 75, 85-86 (1984).

you").[216] If a denizen of cyberspace finds an area in cyberspace offensive, he or she merely refuses to visit that location. The self-help model is usually most effective when there are few or no externalities and the transaction costs in negotiating a contract are high.[217] The absence of externalities ensures that the action is really unilateral; therefore, no third party is either benefitted or harmed by the action, so the rights of third parties do not need to be considered prior to taking the unilateral action.[218] In cyberspace, this model is particularly compelling.[219] The evolution of technology makes self-help rules a feasible option.

a. Spamming[220]

One example of the self-enforcing model occurred on April 18, 1994, when thousands of Usenet users were faced with up to dozens of messages from a law firm that was advertising how to get an Immigration and Naturalization Service green card.[221] Such a crass commercialization of cyberspace met almost universal disapproval.[222] The denizens of cyberspace responded with letters, faxes, and E-mail. The volume of E-mail was so great that it repeatedly crashed the law firm's Internet service provider — promptly disconnecting, in fact, the firms account.[223] The law firm dug in its heels, threatened to sue its ISP, and stated its intention of continuing to advertise on the net.[224] A Norwegian, Arnt Gulbrandsen, created a cancelbot, a program that would automatically delete every message that the firm tried to post on Usenet twenty seconds after it was posted.[225] This enforcement proved an elegant resolution to

---

216 *Id.* at 131 n.21. Self-help with some limitations is recognized in tort law. *See* RESTATEMENT (SECOND) OF TORTS § 201 cmts. I-k (1965); U.C.C. § 9-503 (Unless otherwise agreed, a secured party has on default the right to take possession of the collateral, without judicial process, if this can be done without a breach of the peace.).

217 Hardy, *supra* note 140, at 1017.

218 *Id.*

219 *See* Jerry Berman & Daniel J. Weitzner, *Abundance and User Control: Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media*, 104 YALE L.J. 1619, 1631-34 (1995).

220 Spam—"(From the Monty Python "Spam" song) to post irrelevant or inappropriate messages to one or more Usenet newsgroups or mailing lists in deliberate or accidental violation of netiquette. . . . Posting a message to a significant proportion of all newsgroups is a sure way to spam Usenet and become an object of almost universal hatred." FOLDOC—FREE ON-LINE DICTIONARY OF COMPUTING (visited May 25, 1997) <http://wombat.doc.ic.ac.uk/foldoc/index.html>.

221 STOLL, *supra* note 23, at 104. While the denizens of cyberspace have a strong cultural aversion to advertising, they value information. Companies that want to advertise on the Internet best do it by posting factual information regarding their products on the World Wide Web where the information is only available to those looking for it.

222 *Id.*

223 *Id.*

224 *Id.* at 105.

225 *Id.*

what appeared to be an intractable legal battle — the perfect solution to unwanted advertising on the net. The cancelbot is effective against "spamming" — the posting of a message on multiple Usenet news groups or listserves that is not relevant to the purpose or topic of the list or is commercial in nature.

b. Pornography

More recent examples of technology facilitating self-help remedies are programs that allow parents[226] or employers[227] to control access to the Internet: SurfWatch, Cybersitter, and Net Nanny. In the early 1990s, the Internet shifted from being a primarily academic and research community to becoming a "family" network.[228] As the number of children increased, concern about the nature of the content available in cyberspace increased, and the dangers of the Internet became a popular stalking horse of those who had never visited cyberspace.[229] In response to the reasonable concerns of parents and teachers, software manufactures created programs designed to permit parents and other adults to control which Internet sites and facilities are accessible to children.[230]

---

226 A major critique of screening technologies is that parents are uninterested, disinterested, unwilling, or unable to utilize screening technology to protect their children from age inappropriate content. *See, e.g.*, Robert W. Peters, *There is a Need to Regulate Indecency on the Internet*, 6 CORNELL J. L. & PUB. POL'Y 363, 365-68 (1997) (citing a study that "at least one in four parents were 'basically passive, preoccupied, and downright negligent.'"). Yet, "[i]t is cardinal with us that the custody, care and nurture of the child reside first in the parents whose primary function and freedom include preparation for obligations that the state can neither supply nor hinder." Reno v. ACLU, 1997 WL 348012 at *11 n.31 (quoting Prince v. Massachusetts, 321 U.S. 158, 166 (1944)).

227 Employers have an economic incentive to insure that work-time and employer owned technology is used for "work purposes" only.

228 *See* Molly Ivins, *Congress Goes After Sex on the Internet*, SAN FRANCISCO CHRON., Mar. 31, 1995, at A25 ("Until about 1990, the Internet was designed for adults only."); Elmer-Dewitt, *supra* note 117, at 50 (originally the Internet linked government, educational institutions, and corporations, and until 1993, it was difficult for an ordinary computer user to access the Internet).

229 Steve Wildstrom & Toddi Gutner, *Cybersmut: How to Lock out the Kids*, BUS. WK, Feb. 12, 1996, at 98.

230 *See* Kevin Reichard, *Three Cybersmut Censors Try to Clean Up the Internet. (SurfWatch Software's SurfWatch 1.0v; Solid Oak Software's Cybersitter 1.2; Net Nanny Ltd's Net Nanny 2.0) (First Looks) (Software Review) (Evaluation)*, PC MAG., Nov. 7, 1995, at 46; Bruce Haring, *Efforts to Police Internet*, USA TODAY, June 14, 1995, at 1D. If all of these arrangements sound *ad hoc*, it is because they have mostly sprung up in recent months in response to parental concerns and political pressures. Wildstrom & Gutner, *supra* note 144, at 98.

Cybersitter,[231] Net Nanny,[232] and SurfWatch[233] are a few of the programs that block a PC user's access to offensive materials on the Internet, including World-Wide Web and FTP sites, "alternative" newsgroups, IRC chat rooms, Gophers, and E-mail.[234] Programs are sold to concerned parents and employers, who do not want employees surfing cyberspace during work hours.[235] Some of these programs can also monitor net access on commercial ISP providers such as America On-Line, CompuServe, and Prodigy.[236] "[A] foolproof filter list is impossible to develop because of the subjective nature of what is considered objectionable, as well as the continually changing Internet."[237] The designers of these programs, like Associate Justice Potter Stewart, simply know it when they see it.[238]

Cybersitter is one of the most powerful of these products.[239] Cybersitter blocks access to specific Internet resources (Web, FTP, and Usenet Newsgroups) and censors specific search words.[240] Cybersitter contains a large database of objectionable Internet sites.[241] Because the content of the Internet rapidly changes, Cybersitter allows a parent to log their child's Internet usage and to add specific sites to the database that the parent wants to block.[242]

Net Nanny compares incoming and outgoing text against a dictionary of "banned words" that the parent creates and can also screen for pornographic images.[243] Net Nanny allows parents to customize their own screening list for objectionable content (not limited to just pornogra-

---

231 *Solid Oak Software* (last modified Apr. 16, 1997) <http://www.solidoak.com/cysitter.htm> [hereinafter Cybersitter].

232 *NetNanny* (visited Apr. 24, 1997) <http://www.netnanny.com> [hereinafter Net Nanny].

233 *SurfWatch* (visited Apr. 24, 1997) <http://www.surfwatch.com> [hereinafter SurfWatch].

234 The legal issues raised by these services is beyond the scope of this article. For a general discussion of the legal issues raised by rating services, see Volokh, *supra* note 35, at 429-434.

235 Id. From the employer's perspective this is similar to blocking access to "900" telephone number.

236 *Id.*

237 Kathryn Munro, *PC Magazine Online: Filtering Utilities* (visited Apr. 24, 1997) <http://www.pcmag.com/features/utility/filter/_open.htm>.

238 *See* Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring) ("I know [pornography] when I see it.").

239 Editor's Choice, *PC Magazine Online* (visited Apr. 24, 1997) <http://www.pcmag.com/features/utility/filter/ufuec.htm>.

240 Jay Munro, *PC Magazine Online: Cybersitter* (visited Apr. 24, 1997) <http://www.pcmag.com/features/utility/filter/ufu2.htm>.

241 Cybersitter, *supra* note 231.

242 *Id.*

243 Net Nanny, *supra* note 232, at <http://www.netnanny.com/nnfaq.html> (visited Apr. 24, 1997).

phy)[244] and to direct the software to log the activity or shut down the computer (among other things).[245] *PC Magazine Online* noted that "[w]hen Net Nanny detects a listed violation, it can block access, monitor hits, mask words, or shut down an application — all of which worked well in our tests."[246] Net Nanny can also block images[247] and will provide downloadable lists of specific sites identified by Net Nanny staff.[248]

SurfWatch monitors Internet activity by blocking access to objectionable Web or FTP sites, IRC chat groups, newsgroups, or Gophers.[249] SurfWatch comes with a list of objectionable sites containing indecent or pornographic materials and, for an additional fee, provides monthly maintenance.[250] If a child or employee attempts to access an "objectionable site," SurfWatch denies access and displays a dialog box informing the user.[251]

The Communications Decency Act criminalized knowingly transmitting indecent materials using the Internet to individuals under the age of 18.[252] The statute provided a safe haven for individuals who "require[d] use of a verified credit card, . . . adult access code, or adult personal identification number . . . ."[253] To enable individual content providers to take advantage of this safe haven, services such as Adult Check, Adult Virtual System, First Virtual, Validate, or VeriSign began to perform some sort of "adult verification."[254] Adult Check for example allows individuals or organizations which are concerned that they may be posting indecent material to verify that the viewer is over 18 years of age (or at least that the viewer has access to an Adult Check ID number).[255] One of the initial complaints regarding the CDA was that it imposed financial burdens on the individual seeking to post questionable materials on his or her web site.[256] Adult Check charges the individuals seeking access to the content and pays content providers through a referral sys-

---

244 *Id.*

245 *Id.*

246 Kathryn Munro, *PC Magazine Online: Net Nanny* (visited Apr. 24, 1997) <http://www.pcmag.com/features/utility/filter/ufu4.htm>.

247 Net Nanny, *supra* note 232, at <http://www.netnanny.com/nnfaq.html> (visited Apr. 24, 1997).

248 *Id.*

249 Kathryn Munro, *PC Magazine Online: SurfWatch* (visited Apr. 24, 1997) <http://www.pcmag.com/features/utility/filter/ufu4.htm>.

250 *Id.*

251 *Id.*

252 47 U.S.C.A. § 223 (West Supp. 1997).

253 47 U.S.C.A. § 223(e) (5) (West Supp. 1997).

254 Shea on Behalf of American Reporter v. Reno, 930 F. Supp. 916, 933-34 (S.D.N.Y. 1996), affirmed, 65 USLW 3323 (Jun. 27, 1997).

255 222 (visited Apr. 27, 1997) <http://www2.adultcheck.com/cgi-bin/merchant.cgi?4803>.

256 *Id.*

tem.[257] The web site owner is paid a fee for each referral that leads to a membership in Adult Check.[258] Even not-for-profits can use these systems.[259] Again, this is an example of cyberspace technology permitting self-help.

c. PICS

Finally, PICS (Platform for Internet Content Selection) was developed by the Massachusetts Institute of Technology's World Wide Web Consortium.[260] PICS is an infrastructure for associating labels with Internet content.[261] PICS allows a parent to be sure that when his or her son or daughter is visiting www.playboy.com or www.playgirl.com, he or she is in actually only reading the articles. When a PICS code is embedded into a document, a web browser can scan the document and either display it or reject it depending on the PICS rating and the viewers preferences without the viewer actually seeing the document. Web sites may be rated as a whole or based on individual pages, or even parts of a page.

Although it communicates in a standard language, the individuals rating the web sites do not necessarily share common values; rating services create the common language.[262] In general, there are two types of

---

257 *Id.*

258 *Id.*

259 These programs do not meet the needs of organizations whose goal is to get their message to the widest possible audience free of charge. Also it is not clear that the government could limit access to these Internet sites only to adults who can prove they are "adults." *See Lamont v. Postmaster General of the United States*, 381 U.S. 301, 305 (1965) (holding that a statute requiring post office to detain and destroy foreign mail it considered to be communist propaganda unless the addressee requested to receive the mail an unconstitutional limitation on First Amendment rights). For reasons similar to the court's analysis *Lamont*,

> This requirement is almost certain to have a deterrent effect, especially as respects those who have sensitive positions. Their livelihood may be dependent on a security clearance. Public officials like schoolteachers who have no tenure, might think they would invite disaster if they read what the Federal Government says contains the seeds of treason. Apart from them, any addressee is likely to feel some inhibition in sending for literature which federal officials have condemned as 'communist political propaganda.'

Id. at 306. Individuals in cyberspace may forgo access to constitutionally protected content rather than risk their family, friends, neighbors, or employers discovering membership in an adult identification service, regardless of the nature of the content they choose to access.

260 Resnick, *supra* note 28, at 2.

261 <http://www.w3.prg/pub/WWW/PICS> (visited May 8, 1997). PICS has the potential to do much more. PICS labels could be used for "code signing, privacy, and intellectual property rights management." *Id.*

262 "User-based zoning is also in its infancy. For it to be effective, (i) an agreed-upon code (or "tag") would have to exist; (ii) screening software or browsers with screening capabilities would have to be able to recognize the "tag"; and (iii) those programs would have to be widely available—and widely used by Internet users." Reno v. American Civil Liberties Union, 1997 WL 348012, *14 (O'Connor, J., concurring in the judgment in part and dissenting).

rating services, third-party rating services and self-rating services.[263] CyberPatrol's CyberNOT list, EvaluWeb, and NetShepherd are examples of third-party rating services.[264] A third-party rating service evaluates a web site and rates it according that organization's standards of "good taste."[265] Recreational Software Advisory Council (RSACi), Safe for Kids, SafeSurf, and Vancouver Web Pages are examples of self-rating services.[266] For example, organizations like RSACi have developed on-screen questionnaires to create a shared PICS vocabulary.[267] Individuals may rate the web site, individual pages, or sections of a page based on numerous categories. Viewers can tailor their viewing to Web sites that meet certain preselected standards.

Of course, the viewer surrenders his or her content choices to a *trusted* reviewer,[268] and governments may mandate that each site be rated and mandate the use of software to thwart access to sites that governing regime considers objectionable.[269]

All of these software programs (and those still to come) will vary in scope and effectiveness;[270] but the "first line of defense against Internet porn — whether you want to protect children or office workers — should be an instilled sense of personal responsibility, not reliance on software that may or may not provide enough protection."[271] "A technological solution to a social problem seldom works without a corresponding change in the attitudes."[272] Still, these programs are excellent examples

---

263 <http://www.w3.org/pub/WWW/PICS/raters.html> (visited May 8, 1997).

264 *Id.*

265 *Id.*

266 *Id.*

267 *RSACi FAQ Table of Contents* (visited May 3, 1997) <http://www.rsac.org.faq.html>.

268 *Cf.* Eugene Volokh, *Cheap Speech and What It Will Do*, 104 YALE L.J. 1805, 1815-16 (1995) (discussing the role of reviewers in a world of information overload).

269 The author assumes that the next phase of "lobbying" will be to pressure rating services to be more attuned to each constituency using the rating service or for each group concerned with content to create their own rating service. The author wonders if this may become a selling point, much like the words "Banned in Boston" assured a best seller in the 1960s, e.g., some viewers may screen out *low* nudity, sex, violence, and adult language sites.

270 The contents of the Internet change faster than frequent updates can track, so the programs supplement their bad-site list by watching for words or phrases in the names of sites or newsgroups. This filtering function often produces curious results. All programs have enough built-in intelligence to avoid the kind of absurdity that hit America Online last year when it banned the word "breast" and cut off online discussions of breast cancer and chicken breasts. *See generally* Wildstrom & Gutner, *supra* note 229, at 98.

271 Reichard, *supra* note 230, at 46; *Personal Technology, Watching Out for the Kids*, SEATTLE TIMES, Mar. 10, 1996, at C1 (describing other products).

272 Nimmer, *supra* note 5, at ¶ 1.02[4]. At least on this point, the author is in agreement with proponents of the CDA. *See, e.g.* Peters, *supra* note 226 at 366. "Yet, parental guidance and control are needed to protect children. Technology is not the solution. Its just a tool. The real answer is parenting: Understanding what your children are doing online, talking to them about it, and guiding them." *Id.* (internal quotations, citations, and footnote omitted).

of technology that permits self-help solutions in cyberspace with minimal externalities, minimal cost, and no government involvement.[273]

d. Disconnection Model

Finally, for disputes between ISPs or ISPs and customers, the disconnection enforcement model is an example of self-help in cyberspace.

> The disconnection enforcement model has the following components. The supplier of the network service unilaterally issues a statement declaring the terms of governing access. The statement primarily emphasizes terms that protect the supplier and so it reserves the power to cancel or modify the terms and obligates the suppliers to little. Rather, the statement emphasizes the [other party's] obligations and waives any implied or preexisting . . . rights.[274]

The disconnection enforcement model unplugs the offender.[275] In the case of an individual user, the disconnection is a vertical disconnection from the host system.[276] In case of an offending network, the disconnection is a horizontal disconnection from other networks — a denial of internnectivity.[277]

e. Intellectual Property

A core function of government is the protection of property. In cyberspace, this is intellectual property. The economics of intellectual property in cyberspace may be sufficiently different so that the protection of intellectual property is unnecessary.[278]

> [T]he profit-maximizing price on the Internet may be where marginal revenue equals marginal cost because intellectual property will be cross-subsidized by other products in a manner sufficient to cover the fixed costs

---

273 Another example is Internet Fastforward by Primenet. Fastforward permits the user to access world wide websites without viewing unwanted advertisements. Moreover, many users of cyberspace consider tracking which websites they use for advertising or marketing purposes to be an invasion of their privacy. Fastforward permits a user to delete information regarding his or her visit to the website. *Market Place* (National Public Radio broadcast, May 8, 1996).

Also, listserves and newsgroups (not infrequently) debates and discussions break down into acrimonious flaming. Members then have the option in a moderated list of seeking the assistance of the moderator. If the moderator refuses to intervene or if the list is unmoderated, the individual may join another list or newsgroup.

274 Perritt, *supra* note 36, at 356.

275 *Id.* at 355.

276 *Id.*

277 *Id.*

278 Eric Schlachter, *The Intellectual Property Renaissance in Cyberspace: Why Copyright Law Could be Unimportant on the Internet*, 12 BERKELEY TECH. L.J. 15, 23 (1997).

> associated with intellectual property creation and distribution. If this is true, a market price of zero for intellectual property can still create long-term economic profits attributable to intellectual property creation.[279]

Cross-subsidization could occur through advertising, sponsorships, sales of upgrades, sales of complementary technology or physical goods, services, or through "personal information collection and data mining."[280] If intellectual property is freely alienated then copyright or other protection is superfluous.

But even if a strong regime of intellectual property remains the dominant paradigm in cyberspace, there are self-help options.[281] The software manufacturer could limit technical support to registered users.[282] Authorization codes that would permit the software to function for a limited time.[283] Software envelopes that would contain the copyrighted material and would communicate with the manufacturer on a periodic basis before permitting access.[284] Centralized software available at one location on the net, and the user would pay a fee per use.[285] These intellectual property self-help options are not science fiction. Many of them are already available commericially.[286] With a judicious use of technology and ethical socialization, intellectual property can be protected in cyberspace without resort to government.

2. *Social Control Model (Reputational Sanctions)*

The social control model assumes a voluntary association of Internet users setting rules through social norms or multiparty agreements. The paradigm of social control uses rewards and punishments. Pro-social behavior is rewarded; ordinary social behavior is treated neutrally; and antisocial behavior is punished.[287] Professor Ellickson describes "a system of social control . . . [that] consist[s] of rules of normatively ap-

---

279 *Id.*

280 *Id.* at 22-27; Dyson, *supra* note 32, at 141 ("The real value created by most software companies lies in thier distribution networks, trained user bases, and brand names—not in their code."); *see also* Chon, *supra* note 30, at, 272-76.

281 *Id.* at 38-48 (discussing alternative "self-help" copyright regimes based on technology or contract).

282 Eric Schlachter, *Intellectual Property Protection Regimes in the Ages of the Internet* (visited Apr. 30, 1997) <http://blake.oit.unc.edu/copyright1.html>.

283 *Id.*

284 *Id.*

285 *Id.*

286 *See, e.g., id.* at nn.85 & 87 (providing the URLs for companies producing some of these products).

287 ROBERT C. ELLICKSON, ORDER WITHOUT LAW 124 (1991) (Table 7.1). An example of this system in the employment context is when an extraordinary employee receives a bonus; the ordinary employee receives only his or her expected salary; and the under-performing employee is fired.

propriate human behavior. These rules are enforced through sanctions, the administration of which is itself governed by rules."[288] There are five "controllers" of punishment and rewards.[289] "The five consist of one first-party controller, one second-party controller, and three third-party controllers."[290] A person who imposes rules and sanctions on himself is exercising first-person control.[291] First-person control is "personal ethics."[292] Second-party controllers are contracts.[293] The three types of third-party controllers are social forces (norms), organizations (organizational rules), and governments (law).[294] Voluntary or private associations are created, exist through rules, and tend to be self-governing.[295] These rules may be formal, written rules, or rules based on custom passed on to new members through oral tradition and actual practice.[296] Under the social enforcement model, the "controller is the group as a whole, rather than the state, an individual, or an organization."[297] This section will focus on governing cyberspace through informal social norms, for this model is the most decentralized and democratic.

Some critics may argue that this is not real law;[298] at best it is voluntary compliance with some vacuous community norm. Yet, contract law scholars have long discovered that compliance with contract terms in the business community is relatively unaffected by the ultimate legal enforceabilty of the contract.[299] Business relationships create sanctions. Business people who depart from the accepted norms of behavior in their peer group risk losing business opportunities or status in their community.[300] Finally, we know from extensive study of black markets and

---

288 *Id.* at 124.

289 *Id.*

290 *Id.* at 126.

291 *Id.*

292 *Id.* at 127.

293 *Id.*

294 *Id.* at 127.

295 *Id.*

296 In cyberspace, dissemination of rules is done through *frequently asked questions*, netiquette, and flames.

297 Kornhauser, *supra* note 150, at 651.

298 *See* Perritt, *supra* note 36, at 1022 & n.67.

299 *See* STEWART MACAULAY ET. AL, CONTRACTS IN ACTION 413 (1995).

300 *See id.* at 414. Professor Macaulay recounts an historical example in Essex County, Massachusetts between 1629 and 1692. Allegations of exceeding the just price were serious charges that could harm a merchant whether he was guilty or not. So merchants who heard rumors regarding their integrity would immediately sue for defamation to vindicate their reputations in the community. *See id.* at 573 (quoting KONIG, LAW AND SOCIETY IN PURITAN MASSACHUSETTS: ESSEX COUNTY, 1629-1892). *See also* Eric A. Posner, *The Regulation of Groups: The Influence of Legal and Non-Legal Sanctions on Collective Action*, 63 U. CHI. L. REV. 133 (1996).

criminal enterprises that private governments are quite able to enforce community sanctions.[301]

The social enforcement model uses the social constraint of a cohesive community whose penalties range from truthful negative gossip to excommunication from the community.[302] Cyberspace has been largely governed by an informal set of norms that are enforced through social control.[303] Experienced users inculcated Cyberian values into new-comers.[304] The responses to a breach of "netiquette" range from polite reproof to major flames. The communication is the defining characteristic of cyberspace. So, cyberspace is uniquely suited to governance using social or reputational sanctions. A reputational sanction may be communicated throughout cyberspace in moments.[305] But the anonymous apersonal nature of cyberspace attenuated the effects of such sanctions. In cyberspace, because of anonymous postings and problems of authentication, the reader has no way to determine the credibility of the individual administering the administrative sanction. Further, the recipient of a reputational sanction may just change his name and continue to carry-on so experiencing little or no effect of the sanction. Although the cohesiveness of the Cyberian community has been questioned by some, this ability to create rules and administer sanctions is the basis for self-regulation in cyberspace.

This model, then, exemplifies the preconditions necessary to establish an effective voluntary association — that is, a voluntary association that can self-govern and self-enforce without resorting to outside enforcement mechanisms.[306] Game theory explains why multidimensional relationships are necessary to effectively govern through social norms.[307] The Prisoner's Dilemma demonstrates the basic principles involved.[308]

---

301 *See* MACAULAY, *supra* note 299, at 413.

302 *See generally* ELLICKSON, *supra* note 287.

303 Lemley, *supra* note 104, at 312.

304 Seniority and authority in cyberspace tends to be based on-line experience or individual merit rather than chronological age. *Cf.* Suzanne P. Weisband, et al., *Computer-Mediated Communication and Social Information: Status Salience and Status Differences*, 38 ACADEMY OF MANAGEMENT JOURNAL 1124, 1124 (1995) ("Many studies have found that groups that interact by computer-mediated communication . . . technologies are less prone to domination by high-status members than are face-to-face groups."). The Missouri adage "show me" is frequently the motto in a community where anyone can *aspire* to claim to be anyone or anything. Also, traditional hierarchies break down when access is essentially equal. Lemley, *supra* note 104, at 312.

305 For a fascinating account of the theoretical effect of reputational sanctions in a libertarian community, see Dmitry N. Feofanov, *Luna Law: The Libertarian Vision in Heinlein's the Moon is A Harsh Mistress*, 63 TENN. L. REV. 71, 81 (1995) ("'If a man's word isn't any good, who would contract with him? . . . [P]eople won't speak to you, buy from you, sell to you.'").

306 Perritt, *supra* note 36, at 360.

307 Kornhauser, *supra* note 150, at 659, 663.

308 *Id.* The basic model of the Prisoner's Dilemma is that two individuals are arrested. The government has sufficient evidence to convict both of them of a misdemeanor, but needs

In this game, each player is given two choices: "cooperate" or "defect."[309] In a one shot game, a rational player will maximize the player's welfare by defecting. But players in a continuing game who do not know which "turn" will be the last maximize their individual welfare by cooperating.[310] Multidimensional relationships also assume that there are no gross conflicts between the players — all players are similar situated. Further multidimensional relationships help ensure that the game remains in Nash equilibrium so that no player can unilaterally improve the payoff. Professor Ellickson assumes that a defection by player *JP* in a game between *JP* and *LaFond* may be sanctioned in the next round when player *JP* faces player *Durkee*. *Durkee,* aware of *JP*'s defection, will adopt a defection/defection strategy to minimize loss.[311] The enforcement is social because the tit for tat strategy is enforced by the community of players rather than the innocent victim.[312] The more dimensions of interaction between players, the less likely a player can create a strategy that will result in a unilateral playoff (defection) without a corresponding off-set on another level.

There is some question about the extent to which individuals establish continuing relationships in cyberspace.[313] Howard Rheingold describes vibrant communities in cyberspace.[314] Denizens of cyberspace may have continuing relationships in cyberspace communities. Communities are not just electronically mediated, but in times of crisis or need extend into the "real world." Many CMC communities are laden with back-channel communication. In addition to the exchange on e-mail or messages that is visible to all users, there may be a private exchanges of

---

the assistance of the other prisoner to convict either prisoner of a felony. Each prisoner is interrogated separately and offered a reduced sentence if the prisoner testifies. If one prisoner refuses to testify and the other prisoner testifies, then the prisoner who refuses to testify gets a correspondingly more severe sentence. *See id.* at 659 n.62.

309 *Cooperate* in this situation means comply with the social norm. *Defect* means deviate from the social norm. *See* Kornhauser, *supra* note 150, at 663 n.62.

310 *Id.* at 660 n.67; ELLICKSON, *supra* note 287, at 164-66.

311 Kornhauser, *supra* note 150, at 665-67.

312 This model requires some awareness of reputation; *see id.* Therefore, it seems particularly apt for cyberspace, where information about a user's reputation can be disseminated virtually instantly.

313 Perritt, *supra* note 36, at 360; *but see* Malcolm R. Parks & Floyd Kory, *Making Friends in Cyberspace*, 46 J. COMM. 80 (1996) (Sixty percent of the participants in a study reported that they has formed personal relationships with individuals they first contacted through a newsgroup.); Jacobson, *supra* note 119, at 467;Wellman, *supra* note 26, at 220-22.

314 Perritt, *supra* note 36, at 360. Howard Rheingold describes the Well as a thriving online community with multidimensional relationships. RHEINGOLD, *supra* note 2, at 17-38. Virtual relations may be stronger and more vibrant than "real ones." There are numerous examples of individuals meeting on line and later marrying.

electronic messages, telephone conversations, or even in person meetings to supplement the communication that is visable to the community.[315]

Many Cyberians are tourists; they enter and leave Cyberian communities without any connection to members of that community. The one dimensional nature of some Cyberians' experiences attenuates the effect of social disapproval as a sanction in cyberspace.[316] But more and more tourists are becoming residents. A violator of the rules of a self-governing cyberspace community who is "excommunicated" from the community can locate a new community and create a new identity there. Moreover, considering the relative anonymity in cyberspace, the violator may even rejoin the original community under a new identity.[317] In either case, it takes time and effort to make new friends and to become accepted in the new community—and even there, sometimes one's reputation will follow. Also, many Cyberians develop long term personal relationships in cyberspace that extend to the real world. Anti-social acts in cyberspace can effect real world social interaction.

An example of a virtual crime, trial, and adjudication took place on a MOO.[318] In March 1993, a virtual personality Mr. Bungle used a software tool commonly called a voodoo doll[319] to virtually rape another virtual personality Legba. Later that evening, he also virtually raped another virtual personality Starsinger.[320] The virtual rape took place in a virtual community of LambdaMOO.[321] Mr. Bungle forced two virtual personalities to service him "in a variety of more of less conventional ways."[322] Usually, MOOs and MUDs have superusers called wizards that resolve disputes among the participants. On LambdaMOO, however, the wizards devolved the power of settling disputes to the participants and restricted themselves to the technical hardware and software problems of supporting a MOO.[323] The community was faced with three choices; (1) the legalists argued that nothing could be done because virtual rape was not against the rules in the community; (2) the royalists argued for the return of the wizardocracy; and (3) the

---

315 For example, the author is a member of several electronic conferences for lawyers and law professors. In addition to sharing information in the electronic conferences, members send private e-mail, telephone calls, meet at conferences and symposia, and share common real life friends. The relationships one develops and shares in these electronic conferences is as complex and multideminsional as "real life" relationships.

316 Perritt, *supra* note 36, at 360.

317 Dibbell, *supra* note 107, at 486. In the LambdaMOO incident, community members quickly discovered the "true identity" of the new cybercommunity member. *See id.* at 477.

318 *Id.*

319 A "voodoo doll" is a program that attributes to others actions that the users did not actually write. *See id.* at 475.

320 *Id.* at 473.

321 *Id.* at 474.

322 *Id.* at 473.

323 *Id.* at 479.

technolibertarians argued that the only response was for the individuals who were offended to block the offending messages.[324] However persuasive that argument may be in the normal run of circumstances, here the command would only prevent the virtual victims from experiencing their own cyber-rape while the other members of the community were free to witness the event.[325] While perhaps not a consensus, the LambdaMOO community resolved things after long debate by "toading" Mr. Bungles:[326] eliminating his character from the virtual community.[327]

In response to the Mr. Bungles incident, the wizards put into place a system of petitions and ballots where any member of the LambdaMOO community could put any issue to popular vote and the decision of the community would bind the wizards.[328] Mr. Bungles later tried to return to LamdaMOO as Dr. Jest. However, he faced social ostracism and finally departed permanently from LambdaMOO.[329] This is a clear example of a Cybercommunity creating its own laws, adjudicating a violation of those laws, and punishing violations—acting as a community.

3. *Penology of Cyberspace*

Individuals can be punished in cyberspace through jail,[330] social ostracism, removal from the relevant Cyberian community, and ultimately disconnected from the system by their ISP.[331] After the Cyberian punishment has been inflicted, the individual may still be punished in the real world through the law of the jurisdiction where the user may be found. A study of the "penology" of cyberspace is beyond the scope of this article. Without resort to institutions outside of cyberspace, there are numerous mechanisms to sanction the violation of those rules. Nonetheless, the sanctions discussed so far appear to be effective in meeting all of the three principles that are generally used to justify punishment: protection, deterrence, and retribution.

B. CONTRACTING FOR GOVERNANCE IN CYBERSPACE

In theory, the contract basis for governing cyberspace would result in a seamless web of contractual rights, duties, and enforcement mecha-

---

324 *Id.* at 479.
325 *Id.* at 480.
326 *Id.* at 485.
327 *Id.* at 478.
328 *Id.* at 485.
329 *Id.* at 488.
330 For example on a MUD/MOO, a wizard may take an offending user aside and suspend that person's access to the community while engaging in remedial social instruction. These individuals are often taken to an area in the MUD/MOO called "jail." While in jail, the offender has no social interaction within anyone but wizards.
331 As digital cash becomes more prevalent, fines may become more feasible.

nisms that would bind and build the community and avoid the difficult issues of jurisdiction, international law, comity, and sovereignty.[332] Each user would have a contract with that user's ISP.[333] The ISPs would then have contracts with each other that govern their relationships and the relationships of the ISP's users.[334] For example, user *JP*, who accesses the Internet through *ANET*, has a disagreement with user *LaFond*, who accesses the Internet through *BNET*. JP and LaFond have no contract or formal relationship to resolve their dispute. They will find that when they joined *ANET* and *BNET*, respectively, they agreed to contractual provisions that will govern disputes in cyberspace. *ANET* and *BNET* have a contract that governs disputes between their respective members. The contract between *ANET* and *BNET* may not be directly between themselves, but rather between them as members of an ISP trade association or as common users of a telecommunications company that provides net access.

If the contracts entered into are truly negotiated and represent a meeting of the minds — or, at least, an agreement of the electronic agents — then cyberspace should be governed under the rubric of contract. Individuals should be required to honor agreements they freely entered into. But if the contracts are standard form contracts to which Cyberians will unknowingly assent and waive valuable rights in exchange for access, the potential for abuse is too great. "Speech is regulated . . . under terms of contract that people agree to when they again access to the Internet through [ISPs]."[335] "By first making the contract then by declaring who should construe it, the strong could oppress the weak, and in effect so nullify the law as to secure the enforcement of contracts usurious, illegal, immoral, or contrary to public policy."[336]

Another criticism the contract law approach is that it protects only the contracting parties and those in privity with them. A contract based law of cyberspace could provide third parties with the *option* of seeking protection under the law and adjudication procedures of cyberspace, but

---

332 *See* Dunne, *supra* note 1, at 10-13; Perritt, *supra* note 29, at 25 ("Purely private contact can achieve some immunity from outside legal institutions by waiving application of external law and recourse to external legal systems.").

333 Many users already enter cyberspace through private networks or ISPs, for example America On-Line (AOL), CompuServe, Prodigy, the Well, through colleges, universities, or research institutions with acceptable use policies, and through employers with policies that govern behavior in cyberspace while using employer supplied access. *See* Hardy, *supra* note 140, at 1029-30.

334 Imagine the paradigm of major league baseball that is brought to cyberspace without the all-powerful commissioner. The relationships of owners, managers, players, and umpires are all governed by a web of contracts—even the rules of baseball are a function of contract.

335 Peters, *supra* note 226, at 370 n.58 (quoting David Cay Johnston, *The Fine Print of Cyberspace*, N.Y. TIMES, Aug. 11, 1996, sec. 4, at 5).

336 Parsons v. Ambos, 48 S.E. 696, 697 (Ga. 1904).

it could not force a non-Cyberian to forgo other remedies. Assuming that there is no strong advantage to forum shopping, third-parties will generally find Cyberian adjudication faster and cheaper than resorting to their local courts, where they will face perplexing questions about jurisdiction, venue, and choice of law. This section argues for contract law as the governing paradigm, but urges Cyberians not to shrinkwrap the social contract in cyberspace.

1. *Contracting for a New Social Contract*

The law of cyberspace *may* be established in the marketplace and *may* reflect the will of the participants. Some cyberspace activities may price themselves out of the market.[337] Proponents of the contract model assume that, because of the decentralized nature of the Internet, there will be numerous Internet service providers and the user will always be free to change ISPs.[338] Arguably, the ISP must set competitive terms in order to compete in a competitive market place.[339] Individuals who wish to engage in high risk behavior (for example, potential cybertorts) will join an ISP which will charge more to cover the additional risk. But almost everyone will be able to find an ISP contract with terms that permits him or her the level of access he or she desires. Once a critical mass of ISPs require these standard terms as part of their user contracts or acceptable use policies, other ISPs will follow out of fear that networks that adopt these rules will limit access from non-conforming sites.[340] The individual user will have a contract with his or her ISP; the ISP will have contracts with other ISPs and networks;[341] the networks may contract among themselves. Once the web of contracts are in place, users, ISPs, ISOC, content providers, telcos, and other players have created and assented to the jurisdiction of cyberspace. Finally, the ISPs will act as a

---

337 The market price for some speech or activities may be so high that most market participants may not have an opportunity to purchase the right "to speak" or to engage in these activities. While this drawback would be a marked departure from cyberspace as we currently know it, *see* ACLU v. Reno, 929 F. Supp. 830, 881 (E.D. Pa. 1996), it is not so different from life outside of cyberspace. Just as there are illegal radio stations, one may assume that there may be black or gray-market ISPs to provide access.

338 This flexibility, of course, does not apply to students, employees, or others whose Internet access is conditioned on the use of a particular ISP or whose access to the ISP is based on a "status" such as student or employee.

339 Perritt, *supra* note 36, at 357; Johnson & Marks, *supra* note 144, at 509.

340 Dunne, *supra* note 1, at 13-15.

341 Burnstein, *supra* note 163, at 100:

> For example, AOL and CompuServe might require forum selection clauses in all users' service contracts. In turn, AOL and CompuServe would contract to the effect that disputes arising between an AOL user and a CompuServe user would be governed by a particular forum's law. Following this method, an association of access providers could work in unison to bring much needed certainty to the choice of law issues that will face their users when disputes arise among them.

private legislature that selects through the contract process dispute resolution procedures and provides which forum's laws shall govern the interpretation and enforcement of the contract. This process, therefore, negates thorny national and international jurisdiction and choice of law issues.[342]

2. *Legitimizing a Contract Based Law of Cyberspace*

This market ideal in keeping with the Western democratic goal is to guarantee each person the greatest possible autonomy compatible with equal autonomy for all and the minimum degree of social cooperation that is absolutely necessary to insure society's survival.[343] Such an ideal is in keeping with the origins of cyberspace and the norms and traditions passed on by the first settlers.[344] Professor Dunne describes the original pioneers in cyberspace as "'tend[ing] to be [an] independent, laissez-faire bunch. They put a great store in individualism . . . .'"[345] "Behavior in cyberspace has traditionally been based on a common understanding among its inhabitants about what is acceptable. The Cyberian ethic has been not so much that access to computers should be unlimited and total and that all information should be free, but that this should be so to the extent possible without harming individuals or damaging their property."[346] Accordingly, the contract model of assuring each person the greatest possible autonomy compatible with equal autonomy for all and the minimum degree of social cooperation that is absolutely necessary to insure society's survival fits into the existing cultural norms of cyberspace.[347]

C. SHRINKWRAPPING THE SOCIAL CONTRACT

Not all contracts are open covenants that are openly arrived at. The "shrinkwrap contract" is not unique to cyberspace.[348] The concern with

---

342 Dunne, *supra* note 1, at 9-13. The possible violations of Antitrust law are outside the scope of this article. Suffice it to say, domestic and foreign antitrust regulation must be considered in establishing uniform contracts for cyberspace. *See, e.g.*, Paramount Famous Lasky Corp. v. United States, 282 U.S. 30 (1930) (holding that a requirement that all disputes between motion picture producers and theater owners be arbitrated violated section 1 of the Sherman Antitrust Act).

343 *See* Rosenfeld, *supra* note 33, at 772-73; MACAULAY ET AL., *supra* note 299, at 19.

344 Dunne, *supra* note 1, at 10.

345 *Id.* at 10 (citing Dorothy Denning, *Concerning Hackers Who Break Into Computer Systems* (1990) (paper presented at the 13th National Computer Security Conference, Washington, D.C. Oct. 1-4, 1990)); Burton, *supra* note 2, at 35.

346 Dunne, *supra* note 1, at 10-11.

347 *Id.* at 11 ("Contract's traditional reliance on agreement by the individuals to be bound retains the element of individual responsibility that is an integral part of Cyberian culture.").

348 A shrinkwrap license (contract) is a form of contract that software vendors often try to impose unilaterally on "purchasers" of mass market software. The "purchaser" of the software theoretically "consents" to the terms of the license by opening the plastic wrapping on the

using an authoritarian contract model was first expressed by Professor Friedrich Kessler in 1943:

> Freedom of Contract enables enterprisers to legislate by contract and, what is even more important, to legislate in a substantially authoritarian manner without using the appearance of authoritarian forms. Standard contracts in particular could thus become effective instruments in the hands of powerful industrial and commercial overlords enabling them to impose a new feudal order of their own making upon a vast host of vassals.[349]

The standard form contact is pervasive in modern commercial practices,[350] and has been a common commercial practice for at least the past 100 years.[351] Since the late 1980s, the shrinkwrap or boxtop license has been the license model used for software contracts.[352] Standard form contracts are a result of the hierarchical structure of business organizations and the need to engage in mass volume contracting.[353] Standard

---

software (e.g., the shrinkwrap packaging). Lemley, *supra* note 104, at 311 n.5. The contract is offered on a take-it-or-leave-it basis.

349 Friedreich Kessler, *Contracts of Adhesion — Some Thoughts about Freedom of Contract*, 43 COLUM. L. REV. 629, 640 (1943). Professor Black observed that:

> The contract law system . . . serves massively and systematically as an *intensifier* of economic advantage and disadvantage. It does this because people and businesses who are in strong bargaining positions, or who can afford expensive legal advice, can and epidemically do exact of necessitous and ignorant people contractual engagements which the general law never would impose.

Charles L. Black, Jr., *Some Notes on Law Schools in the Present Day*, 79 YALE L.J. 505, 508 (1970) (emphasis in original). As the contract model is being considered as a basis for law in cyberspace, one should also remember that it was one of the legal underpinnings of feudalism.

350 Eric Mills Holmes & Dagmar Thurmann, *A New and Old Theory for Adjudicating Standardized Contracts*, 17 GA. J. INT'L & COMP. L. 323-24, 334 (1987).

351 *Id.* at 325-26. *See also* W. David Slawson, *The New Meaning of Contract: The Transformation of Contracts Law by Standard Forms*, 46 U. PITT. L. REV. 21, 31 (1984).

352 Until *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996), it was generally accepted that shrinkwrap licenses were not enforceable. *See* Step-Saver Data Sys., Inc. v. Wyse Tech., 939 F.2d 91 (3d Cir. 1991); Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 268-70 (5th Cir. 1988); Arizona Retail Sys., Inc. v. Software Link, Inc., 831 F. Supp. 759 (D. Ariz. 1993); Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239, 1263 & n.107 (1995); *but see* Robert W. Gomulkiewicz & Mary L. Williamson, *A Brief Defense of Mass Market Software License Agreements*, 22 RUTGERS COMPUTER & TECH. L.J. 335 (1996). The Seventh Circuit's opinion in *ProCD*, revived the debate. Regardless of whether shrinkwrap licenses are enforceable under existing law, they will be enforceable in the states that adopt proposed Article 2B to the Uniform Commercial Code. *See, e.g.* §§ 2B-307-309.

353 Holmes & Thurmann, *supra* note 350, at 334.

form contracts allow "numerous, relatively detailed contract[s],"[354] reduce transaction costs,[355] and "assure uniformity and quality."[356]

The shrinkwrap model assumes that the Internet service provider unilaterally establishes rules for use and access, methods of adjudication, and enforcement.[357] The ISP unilaterally, without negotiation, and without considering the rights of the user, offers terms which protect the ISP.[358] Further, the ISPs reserve the right to unilaterally modify the terms in the future and contain de minimis obligations to the user.[359] The user need not be aware of the changes in the terms. For example, the ISP could announce during the log-on process that there are new changes to the terms of service, and if the user would like the read them, the user could access a special file. If the user does not object within some specific period, the user automatically "agrees" to the new terms.

The disadvantage is that such rules are made secretly and presented to the user on a take-it or leave-it basis.[360] Each institution involved in providing Internet services to the public faces similar economic, political, and legal constraints. As rational profit-maximizing institutions, they will draft contracts that maximize their legal rights, minimize their legal obligations, and whenever possible, shift their potential liability.[361] "If a standard form contract clause's validity should be challenged . . . and held unenforceable, the ISP suffers nothing. Similarly the ISP is no worse off than if the unenforceable clause had not been in the contract in the first place (and of course, might be much better off if the interim effect of the clause staved off other individuals' legal claims)."[362]

---

354 *Id.*

355 *Id.*

356 *Id.* Uniformity and quality is assured because the customer is not permitted to dicker for different terms and employees of the seller are (or should be) aware of the obligations of their employer.

357 Perritt, *supra* note 36, at 354. ISPs are the point of entry for all denizens in cyberspace. Thus, they are the most logical points to govern cyberspace. Professor Perritt notes that host-based electronic networks already use the authoritarian model. *Id.* at 354 n.13. For example, commercial information services provide written contracts that are supplemented by notices which appear on user screens. *See id.* Generally, the user accepts or rejects the supplemental terms by typing the "y" key (yes) or "n" key (no). *See id. See also* Johnson & Marks, *supra* note 144, at 488-89.

358 Perritt, *supra* note 36, at 356.

359 *Id.*

360 This article assumes that technology will be unable to compensate for the potential evils of the shrinkwrap license.

361 Lawyers tend to draft standard form contracts to the "edge of the possible," i.e., the maximum latitude allowed by law, in order to protect a client from every *imaginable* contingency. William T. Vukowich, *Lawyers and the Standard Form Contract System: A Model Rule that Should Have Been*, 6 GEO. J. LEGAL ETHICS 799, 827 (1993); Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1172, 1222, & 1244 (1984).

362 Vukowich, *supra* note 361, at 828.

Because these institutions provide Internet services in a common regulatory and economic environment, the contracts will be substantially similar and agreements between these institutions will ultimately shift liability to the individual user.[363]

In essence, this process creates a collective private legislature.[364] However, no one elected the members of this legislature; it is not accountable to anyone, and there are no ways to amend the legislation.[365] The proponents of the contract law model presume an open marketplace that is replete with savvy, sophisticated consumers who will vote with their feet when the terms and conditions of the contract are too onerous.[366] Thus, open market forces will keep the ISP or content provider's unilateral contracts from being too draconian.[367] This view of the market does not reflect existing experience in other market contexts.[368] There may be significant transaction costs in researching and changing to alternative ISPs.[369] "If access requires using a commercial service, and if all commercial services use the same shrinkwrap license, the result is a world that gives 'freedom of contract' to [ISPs] (who wrote the con-

---

363 Compare the collection of ISP Acceptable Use Policies collected at <http://spam.abuse.net/spam/aup.html> (visited June 4, 1997).

364 Lemley, *supra* note 104, at 319.

365 *Id.* at 320.

366 Johnson & Marks, *supra* note 144, at 488-89. For example, United States courts have rejected this argument in the antitrust context:

> [T]here likely will be some large volume, sophisticated purchasers who will undertake the comparative studies and insist, in return for their patronage, that Kodak charge them competitive lifecycle prices. Kodak contends that these knowledgeable customers will hold down the package price for all other customers. There are reasons, however, to doubt that sophisticated purchasers will ensure that competitive prices are charged to unsophisticated purchasers, too. As an initial matter, if the number of sophisticated customers is relatively small, the amount of profits to be gained by supra competitive pricing in the service market could make it profitable to let the knowledgeable consumers take their business elsewhere. More importantly, if a company is able to price discriminate between sophisticated and unsophisticated consumers, the sophisticated will be unable to prevent the exploitation of the uninformed.

Eastman Kodak Co. v. Image Tech. Serv., Inc., 504 U.S. 451, 475 (1992).

367 *But see* Rakoff, *supra* note 361, at 1220-29 (explaining why standard form contracting is not responsive to market forces).

368 *See* Marc Galanter, *Why the "Haves" Come Out Ahead: Speculations on the Limits of Legal Change*, 9 L. & SOC'Y REV. 95, 123-24 n.74 (1974); *cf. Eastman Kodak Co.*, 504 U.S. at 472-75.

369 Perritt, *supra* note 36, at 357; Gerard J. Lewis, Jr., Comment, Lotus Dev. Corp. v. Paperback Software Int'l: *Broad Copyright Protection for User Interfaces Ignores the Software Industry's Trend Toward Standardization*, 52 U. PITT. L. REV. 689, 693 n.11 (1991) ("Training people to use software programs is the largest investment associated with operating computers."). *Cf. Eastman Kodak Co.*, 504 U.S. at 474-75 ("[E]ven if consumers were capable of acquiring . . . [the] information, they may choose not to do so. Acquiring the information is expensive. If the costs of service are small . . ., or if consumers are more concerned about equipment capabilities than service costs, they may not find it cost efficient to compile the information.").

tracts), but none to . . . users."[370] Freedom to change ISPs may be illusory.[371] Users may make substantial investments in hardware and software that may only be compatible with one service provider, and high transaction costs such as obtaining information, negotiation, and reducing the negotiations to an agreement often render a contract based solution economically irrational.[372]

The nature of cyberspace makes it possible to reject traditional principles of standard form contracts in favor of contracts which are freely bargained for and to which the parties freely agree. The major advantage of the standard form contract is that of reduced transaction costs. While this may be an advantage in the real world, cyberspace technology already is reducing transaction costs. For example, the string of email messages exchanged as part of the information and negotiation process also contain the terms of the agreement.[373] Further, the drafts of proposed Article 2B of the Uniform Commercial Code provide for an "electronic agent."[374] An electronic agent is "a computer program designed, selected, or programmed by a party to initiate or respond to electronic messages . . . without review [by] an individual."[375] Article 2B provides that electronic agents may form contracts,[376] make offers, and accept terms.[377] Transaction costs for contracts in cyberspace may be reduced to sending out a "bot" or a "spider" to search the Internet, make offers, and seek acceptances.[378] Accordingly, the one-size fits all contract should be rejected because it is ill-fitted to cyberspace.

D. JUSTICE THROUGH CONTRACT

A community that lacks a "practical agreement on a conception of justice must also lack the necessary basis for political community."[379] Cyberspace is inhabited by representatives of numerous nations and cul-

---

370 Lemley, *supra* note 104, at 320. Critical Legal Studies scholars observe:

> [O]rganizations that engage in repeated standardized transactions can plan these relationships to their advantage. . . . Most individuals are not aware of what they are giving away when they sign. If they were, they would have what one taking the radical position would call little *real* choice but to sign away their rights.

MACAULAY ET. AL, supra note 299, at 11.

371 *Eastman Kodak Co.*, 504 U.S. at 472-75.

372 Hardy, *supra* note 140, at 1017.

373 *See* Ethan Katsh, *Law in a Digital World: Computer Networks and Cyberspace*, 38 VILL. L. REV. 403 (1993).

374 U.C.C. § 2B-102(13) (1996) (draft).

375 *Id.*

376 *Id.* § 2B-202(a).

377 *Id.* § 2B-204(c).

378 For examples of "existing" electronic agents, see Netbot <http://www.netbot.com> and BargainFinder Agent <http://bf.cstar.ac.com/bf>.

379 Alasdair MacIntyre, *After Virtue, reprinted in* WHAT IS JUSTICE? CLASSIC AND CONTEMPORARY READINGS 322 (Robert C. Solomon & Mark C. Murphy eds., 1990).

tures, each with its own definition of justice. Contract permits each community in cyberspace to define its own concept of justice. Therefore, the convergence between law, justice, and contract is also relevant in the context of private law-making or legislation between individuals (i.e. private contracts).[380] In a society which promotes individual autonomy, justice *may be* defined as keeping one's agreements — in essence, *contract as justice*.[381] This approach to defining social norms of behavior is that justice is accomplished without any authority imposing its view of social good on unwilling individuals.[382] In a society which operationally defines justice as a function of contract, no one may force his or her views on others. Nor can anyone be compelled to do anything that he or she has not previously agreed to do.[383] Therefore, the only just institutions are those that are agreed upon by each member of society.[384]

But, the justice of private contracts is raised each time there is a dispute concerning whether society should enforce the contract or provide a remedy for its breach.[385] The justice of a contract between two individuals exists either because the parties *reached a genuine agreement* or because of *the actual terms of their agreement* are just.[386] If the parties have reached a meeting of the minds, the contract is *intrinsically* just because it expresses the will of both parties; therefore, the greatest possible freedom of contract is permitted.[387] The justification of contract law is that contracts are intrinsically just and not premised on any particular vision of what is moral or immoral.[388] The justice of a contract depends on reaching a genuine agreement (i.e., the meeting of the minds *or* the actual terms of the agreement).[389] *Arguendo,* when the consumer is presented with a take it or leave it shrinkwrapped standard form contract, there is no meeting of the minds. Further, consumers may be forced to agree to unconscionable terms under duress as access to cyberspace be-

---

380 *Id.*

381 Rosenfeld, *supra* note 33, at 771 (citing J. LUCAS, ON JUSTICE 208 (1980)). "We are told that Contract, like God, is dead." GRANT GILMORE, THE DEATH OF CONTRACT 3 (1974). But the more appropriate quote in this context may be "God is dead — Nietzsche Nietzsche is dead—God" or the "King is dead, Long Live the King" in this context. As Professor Gilmore was delivering a series of lectures announcing the death of contract, GILMORE, *supra*, at ix, Professor Rawls was enshrining contract as the definition of justice, JOHN RAWLS, A THEORY OF JUSTICE 11-12 (1971). Contract was never able to rest in peace.

382 Rosenfeld, *supra* note 33, at 771.

383 *Id.*

384 *Id.*

385 *Id.* Promisees can enforce contracts without the assistance of the state. *See, e.g.*, Benjamin Klein & Keith B. Leffler, *The Role of Market Forces in Assuring Contractual Performance*, 89 J. POL. ECON. 615 (1981). *See also* Morris R. Cohen, *The Basis of Contract*, 4 HARV. L. REV. 553, 571-85 (1933) (discussing justifications for contract law).

386 Rosenfeld, *supra* note 33, at 771-72.

387 *Id.*

388 *Id.*

389 *See infra* Part VI.B.

comes a necessity rather than a luxury. Because there will not be a genuine agreement, the justice of the contract will have to be evaluated based on the intrinsic terms of the agreement.[390] Two options are readily possible: (1) case-by-case adjudication of the terms of each contract under traditional principles of contract law;[391] or (2) some regulatory agency that reviews these contacts as tariffs — a paradigm similar to the public regulatory model.[392] Since the purpose of self-regulation is to avoid formal governmental structures, issues of fairness should be submitted to arbitration.

VII. ADJUDICATION IN CYBERSPACE-PUBLIC OR PRIVATE "COURTS OF JUSTICE"

After a law of cyberspace is established, disputes will arise that must be adjudicated. Two traditional sources of adjudication are the public courts of a nation and private courts created by contract. Questions regarding choice of law, forum, venue, and jurisdiction render the public law courts inefficient in cyberspace. The contract law model provides a simple solution for resolving disputes in cyberspace—*arbitration*. Unlike private courts, "government" courts are obligated to apply the law of the nation state.[393] This includes national choice of law rules.[394] "According to the traditional and still prevailing view, these conflict of law rules restrict the choice of the law(s) application to international contracts to the law(s) of (a) State(s), to the exclusion of any supra-national or a-national normative system."[395] So even if the contracting parties expressly reference UNIDROIT, UCC, or other default principles (sources) of contract law, national courts will interpret the contract as merely incorporating those additional terms.[396] The proper

---

390 *See* Melvin Aron Eisenberg, *The Bargain Principle and its Limits*, 95 HARV. L. REV. 741, 743-54 (1982).

391 *See* U.C.C. § 2B-308(b)(1) (1996) (draft):

> [A] term does not become part of the contract if the term creates an obligation or imposes a limitation on the party who did not prepare the form: (1) that [is not consistent with customary industry practices at the time of the contract and which] a reasonable [person in the position of the party proposing the form should know would cause an ordinary and reasonable person in the position of the party receiving the form] to refuse the [contract] if that term were brought to the attention of that party.

392 *See* Perritt, *supra* note 29, at 27 ("Contract terms posted in some formal way and subject to review or challenge might be presumptively valid, but not otherwise.").

393 MICHAEL JOACHIM BONELL, AN INTERNATIONAL RESTATEMENT OF CONTRACT LAW: THE UNIDROIT PRINCIPLES OF INTERNATIONAL COMMERCIAL CONTRACTS 120-21 (1994).

394 *Id.*

395 *Id.* at 121.

396 *Id.*

law governing the contract will be determined by the private international law of the forum.[397]

In contrast, arbitrators draw their authority and source(s) of law from the contract so they are "not necessarily bound to base their decision on a particular domestic law."[398] Further, under recognized arbitral principles of *amiable compositeur* and *ex aequo et bono*,[399] if permitted under the arbitration clause,[400] arbitrators are free to fashion a just remedy.[401] This may include the application of supra-national or a-national normative systems to the dispute or looking to existing customs of cyberspace in resolving disputes. Thus, arbitrators, unlike judges, are free to effectuate contracting parties' choice of substantive "law," procedure, and forum in adjudicating the dispute to achieve a just result.[402]

Arbitration is a well established method of resolving contractual disputes. The use of contract in conjunction with arbitration permits the parties to avoid questions of jurisdiction, choice of law, venue, etc. Arbitration permits the dispute to be resolved by arbitrators who are denizens of cyberspace and who are versed in its technology, customs, and traditions. These arbitrators will likely be individuals who are well respected in the Cyberian community. Each constituent community in cyberspace would be free to develop its own customs and law enforced through arbitrators who are familiar with that community. Such arbitrators are likely to resolve disputes in a manner that is acceptable to the parties, to give appropriate weight to the public policy issues, and to develop a law of cyberspace in the arbitral award.

Arbitration is also relatively inexpensive *vis-a-vis* litigation in traditional courts; procedures may be created that fully utilize the flexibility of cyberspace technology, and because arbitration is a well established method of resolving disputes, there are existing "real world" mechanisms

---

397 *Id.* at 122.

398 *Id.* at 124-26.

399 "The . . . two terms—*amiable compositeur* and *ex aequo et bono* authorize the arbitrator to depart from the application of the law in terms of what is regarded as just or equitable under the circumstances. Both terms are used because they had different connotations in various national legal systems." Duane W. Krohnke, *Decisions Standards Raise Policy Issues as Minnesota Drafts an ADR Code of Ethics*, 15 ALTERNATIVES TO HIGH COST LITIG. 3, 6 (Jan. 1997) (citing M. PELLONPAA & D. CARON, THE UNCITRAL ARBITRATION RULES AS INTERPRETED AND APPLIED: SELECTED PROBLEMS IN LIGHT OF THE PRACTICE OF THE IRAN—UNITED STATES CLAIMS TRIBUNAL, 93-95 (1994)).

400 *See, e.g.* Art. 29(3), AAA International Arbitration Rules ("The tribunal shall not decide as amiable compositeur or ex aequo et bono unless the parties have expressly authorized it to do so.").

401 *See* Alejandro M. Garro, *The Contribution of UNIDROIT Principles to the Advancement of International Commercial Arbitration*, 3 TUL. J. INT'L & COMP. L. 93, 114-15, 128 n. 98 (1995); Karyn S. Weinberg, Note, *Equity in International Arbitration: How Fair is "Fair"? A Study of Lex Mercatoria and Amiable Composition*, 12 B.U. INT'L L.J. 227, 240 (1994).

402 Garro, *supra* note 401, at 124-26.

to enforce arbitral awards on both domestic and foreign jurisdictions.[403] Accordingly, the arbitration model is most likely to produce decisions that are accepted by Cyberians as legitimate and by the real world as enforceable.

Because arbitration is a creature of contract law, the parties' submission and the contract circumscribes the scope of the arbitrator's jurisdiction and the arbitrator's ability to fashion a remedy; therefore, arbitration suffers from the same inherent danger of "overreaching" by the stronger or more sophisticated party, if standard form contracts are used to provide for arbitration.[404] However, this article offers only a general *caveat*. Otherwise, these questions in the *arbitral context* are beyond its scope.

A. THE VIRTUAL MAGISTRATE PROJECT

Currently, there are several attempts at pilot projects to resolve disputes in cyberspace.[405] The Online Ombuds Office[406] and Virtual Magistrate Project[407] are two of the better known pilot projects. The Online Ombuds Office does not adjudicate disputes; rather, it serves as a mediator that assists the disputants in resolving the conflict. Because the Online Ombuds Office does not issue rulings, this section will consider the Virtual Magistrate Project in detail.

The Virtual Magistrate Project (VMP) possibly provides the initial footsteps towards dispute resolution in cyberspace, which hopes, through the persuasive force of the magistrates's well reasoned arbitral awards, the VMP will eventually evolve into a law of cyberspace. The VMP was developed in 1995.[408] The VMP anticipates that disputes in cyberspace

---

403 *See* Federal Arbitration Act §§ 1-15, 9 U.S.C. §§ 1-14 (1992); Act of July 31, 9 U.S.C. §§ 201-208 (1992); Convention on the Recognition and Enforcement of Foreign Arbitral Awards, June 10, 1958, 21 U.S.T. 2517, 1958, (*reprinted in* 9 U.S.C.A. §§ 201-08 (West 1992)) (95 countries are signatories to this convention); Michael H. Strub, Jr., Note, *Resisting Enforcement of Foreign Arbitral Awards under Article V(1)(e) and Article VI of the New York Convention: A Proposal for Effective Guidelines*, 68 TEX. L. REV. 1031, 1036 (1990).

404 *See generally* Mark E. Budnitz, *Arbitration of Disputes Between Consumers and Financial Institutions: A Serious Threat to Consumer Protection*, 10 OHIO ST. J. ON DISP. RESOL. 267 (1995); Thomas E. Carbonneau, *Arbitral Justice: The Demise of Due Process in American Law*, 70 TUL. L. REV. 1945 (1996); James L. Guill & Edward A. Slavin, Jr., *Rush to Unfairness: The Downside of ADR*, 28(3) JUDGES' J. 8 (1989); Kronstein, *supra* note 38.

405 Both projects are funded by The National Center for Automated Information Research (NCR), cooperate with each other, and make cross referrals, if appropriate.

406 *See Online Ombuds Office* (visited Apr. 24, 1997) <http://www.ombuds.org>.

407 *See Virtual Magistrate Project* (visited Apr. 24, 1997) <http://vmag.law.vill.edu:8080/>; *see also* George H. Friedman, *Internet & Alternative Dispute Resolution: A Match Made in Cyberspace*, 2(9) MULTIMEDIA STRATEGIST 6 (1996). For a general discussion of the VMP, see George H. Friedman & Robert Gellman, *An Information Superhighway "On Ramp" for Alternative Dispute Resolution*, 68 N.Y. ST. B.J. 38 (1996).

408 *See Virtual Magistrate Project: Frequently Asked Questions* (visited Dec. 20, 1995) <http://www.vmag.law.vill.edu:8080/> [hereinafter *Frequently Asked Questions*].

will involve users of on-line systems, systems operators, and claims of injury that are caused by wrongful messages, postings, and files.[409] The project takes advantage of the unique characteristics of the Internet. As a global dispute resolution service existing solely in cyberspace, it can resolve disputes without having to work within the laws of any particular jurisdiction.[410] The VMP provides for fast, accessible, inexpensive, informal, temporary resolution of on-line disputes.[411] The VMP will provide dispute resolution services globally if the parties agree to have the dispute resolved by the virtual magistrate.[412] The VMP is committed to maximum public availability about information on its decisions and activities.[413] The Cyber Law Institute directs policy for the VMP.[414] The American Arbitration Association administrates all cases submitted to the Virtual Magistrate.[415] The Villanova Center for Information Law and Policy operates the Virtual Magistrate Service,[416] and the NCR provides its funding.[417]

B. GOALS OF THE VMP

The goals of the VMP are to determine whether on-line resolution of on-line disputes is practicable; provide system operators with neutral and expert opinions that respond to claims of wrongful postings; lay the groundwork for a self-sustaining on-line dispute resolution system; define the reasonable response of a system operator who is faced with a complaint; explore whether the VMP could be extended to resolve other grievances in the on-line world; and develop a formal structure for a permanent Virtual Magistrate program.[418]

C. SUBJECT MATTER OF THE VMP

A Virtual Magistrate may adjudicate almost any on-line problem. The scope of the Virtual Magistrate's jurisdiction seems to be focused on content and intellectual property issues.[419] A virtual magistrate has subject matter jurisdiction over complaints about copyright or trademark in-

---

409 *Id.*

410 Whether it is possible to have a-national arbitration without reference to either a situs or the *lex loci arbitri* that produces an enforceable arbitral award is questionable. *See* Hans Smit, *A-National Arbitration*, TUL. L. REV. 629 (1989).

411 *Frequently Asked Questions*, *supra* note 408.

412 *Id.*

413 *Id.*

414 *See Virtual Magistrate Project: Concept Paper* (visited Feb. 26, 1996) <http://www.vmag.law.vill.edu:8080/> [hereinafter *Concept Paper 1*].

415 *Id.*

416 *Id.*

417 *Id.*

418 *Id.*

419 *Id.*

fringement, misappropriation of trade secrets, defamation, fraud, deceptive trade practices, inappropriate materials (obscene, lewd, or material that otherwise violates system rules), invasion of privacy, and other wrongful content.[420] A virtual magistrate may also consider whether it is appropriate for a system operator to deny user access to an on-line system.[421]

D. JURISDICTION OF THE VMP

A virtual magistrate only has jurisdiction over parties who agree to have him or her arbitrate the dispute.[422] The Virtual Magistrate process is voluntary, and his or her power to review a dispute and fashion a remedy is strictly governed by the agreement of the parties. The parties choose which issues to submit to the magistrate and the scope of the magistrate's power to fashion a remedy.[423] However, as with other arbitration proceedings, the magistrate does have some inherent powers once the issue is submitted.[424] The magistrate has no means or power to enforce his award ("judgment"). But arbitration decisions are frequently recognized and enforced by courts throughout the world.[425] Individuals participating in this process should realize that a virtual magistrate's decision has "teeth" and may be enforceable in real courts.[426] Unlike real courts, the decisions by the magistrate are not subject to appeal,[427] but the parties may request that the magistrate reconsider a decision.[428]

The VMP presumes that system operators will, through *standard user contracts*, require that disputes be referred to the Virtual Magistrate — including disputes between users.[429] For example, a term in a standard user contract may require users to resolve any dispute in cyberspace through a virtual magistrate's condition of access. Individual users, sysops, or third-parties may refer disputes on an *ad hoc* basis. In

---

420 *See Virtual Magistrate Project Concept Paper* (visited Feb. 26, 1996) <http://www.vmag.vclip.org:8080/docs/vmpaper.html> [hereinafter *Concept Paper 2*].

421 *See generally Frequently Asked Questions*, *supra* note 408.

422 *Id.* An arbitration is a proceeding to settle a dispute where two or more parties having an interest in the dispute submit the issue for determination to an individual or group (the arbitrator(s)). Unlike a court, the power of the arbitrator is not derived from the government but rather from the consent of the private parties who submit the issue to arbitration. An arbitration clause derives its power from two sources: (1) the agreement of the parties submitting the issue to arbitration; and (2) the power of the government which enforces legal processes. *See* Strub, *supra* note 403, at 1035 n.28.

423 *Frequently Asked Questions*, *supra* note 408.

424 *Id.*

425 *Id.*

426 *Id.*

427 *Concept Paper 1*, *supra* note 414.

428 *Id.*

429 As discussed earlier, standard form contracts are an inherently dangerous basis on which to create law or justice.

cases involving third-parties, for example, the VMP will request that the third party consent to jurisdiction.[430] Over time, with the establishment of an industry-wide protocol that provides for the use of alternative dispute resolution techniques to resolve disputes, there may be a contractual agreement between parties (subscribers and providers) to submit disputes to the virtual magistrate.[431]

E. CHOICE OF LAW OF VMP

In reaching a decision, a magistrate may consider network etiquette, applicable contracts, and appropriate substantive laws without automatically applying the law of any specific legal jurisdiction.[432] The magistrate will consider the circumstances of each complaint, the views of the parties about applicable legal principles and remedies, and the likely outcome in any ultimate litigation or dispute resolution.[433] Decisions of one magistrate will not necessarily be treated as binding precedent for other cases; however, the parties to an arbitration proceeding will be bound by the decision and may not relitigate the identical matter through the Virtual Magistrate. Eventually through the persuasive force and weight of well reasoned arbitral opinions, a body of customary law may develop.[434]

F. THE VIRTUAL MAGISTRATES

The American Arbitration Association and a subcommittee of the fellows of the Cyberspace Law Institute select the magistrates. Therefore, it follows that they are not "real judges" with the power of a government organization behind their awards. Magistrates are paid volunteers who offer their services to resolve disputes in cyberspace.[435] A single magistrate is selected randomly from a pool of qualified and trained arbitrators.[436] Sometimes a case may be referred to a panel of three arbitrators.[437]

Magistrates are required to be familiar with the Virtual Magistrate Rules, the Virtual Magistrate Handbook for Magistrates, the American Arbitration Association Commercial Arbitration Rules, and the American Arbitration Association Code of Ethics for Arbitrators in Commercial

---

430 *Concept Paper 1*, *supra* note 414.

431 *Frequently Asked Questions*, *supra* note 408.

432 *Concept Paper 1*, *supra* note 414.

433 *Id.*

434 There is no reason that the VM's award could not be final so that the matter could not also be relitigated in the courts.

435 *Frequently Asked Questions*, *supra* note 408.

436 *Concept Paper 1*, *supra* note 414.

437 *Id.*

Disputes.[438] Magistrates must be knowledgeable about the law and online systems.[439] Magistrates must comply with a code of conduct that requires neutrality and provides for recusal from cases where they may be perceived to have an interest.

G. PROCEDURE

To commence a proceeding before a magistrate, a complaint must be filed by e-mail.[440] Currently, there is a $10 filing fee to discourage frivolous filings.[441] The complaint should describe the nature of the disputed activity or conduct and the identity of all the parties.[442] Optimally, the complaint will contain: (1) the name, affiliation, address, and electronic mail address of the complainant(s), system operator(s), or other relevant individuals; (2) a description of the disputed action, posting, or conduct; (3) the nature of the objection; and (4) copies of relevant materials.[443] Any participating party may, with the permission of the magistrate, proceed without revealing the identity of a participant.[444] Also a complainant may request that the complaint remain confidential.[445] Once a complaint is filed, the AAA staff reviews it to ensure that the complaint is complete before accepting it and referring it to a magistrate.[446] Each case is assigned its own listserv/newsgroup called a "grist."[447] The magistrate and the participants are registered to the grist and receive all messages posted to it.[448] Submissions from the parties and communications from the magistrate are sent through the grist.[449] All messages sent through are captured and saved at the Villanova Center for Information Law and Policy. While the case is being considered, the parties may access the messages through the docket system on the World Wide Web.[450] The goal of the project is to decide cases within three days. However, the parties are free to agree upon a different time schedule.[451] The magistrate will not make the complaint public until a decision is reached.[452] The parties to a complaint are not prohibited

---

438 *Virtual Magistrate Project: Virtual Handbook for Magistrates* (visited Feb. 26, 1996) <http://www.vmag.law.vill.edu:8080/> [hereinafter *Virtual Handbook*].

439 *Concept Paper 1*, *supra* note 414.

440 *Frequently Asked Questions*, *supra* note 408.

441 *Id.*

442 *Id.*

443 *Id.*

444 *Id.*

445 *Id.*

446 *Virtual Handbook*, *supra* note 438.

447 *Id.*

448 *Id.*

449 *Id.*

450 *Id.*

451 *Id.*

452 *Frequently Asked Questions*, *supra* note 408.

from discussing their participation during this period.[453] If a complaint or a response to a complaint contains confidential information, then the Magistrate may decide that the information can be withheld.[454] Parties that have access to confidential information will be required to abide by confidentiality rulings.[455] All decisions are public.[456]

VIII. FACT-FINDING IN CYBERSPACE

While existing laws and contract paradigm may provide a sound legal basis on which to build an arbitral dispute resolution regime in cyberspace, it is not clear that existing technology lends itself to sound decision making processes.[457] If disputes in cyberspace are essentially requests for the arbitrator to rule on "summary judgment" motions, *i.e.* there is no dispute of material fact so that it is merely a question of what are the legal rights of the parties, then Computer Mediated Communications (CMC) may not affect the adjudicatory process. But, if questions of credibility must be resolved and the arbitrator must make findings of fact then the old adage that "the medium is the message"[458] takes on a special significance. Perhaps, the best historical example of this point of "the medium *creating* the message" is the 1960 Richard M. Nixon v. John F. Kennedy Presidential debates.[459] Individuals who heard the debates on the radio thought that then-Vice-President Nixon won, while individuals who watched the debates on television thought that then-Senator Kennedy won the debate.[460] Some scholars consider the Nixon-Kennedy debates as the defining moment of the 1960 presidential elec-

---

453 *Id.*

454 *Id.*

455 *Id.*

456 *Id.*

457 Further, future teleconferencing and other technological innovations may render these concerns moot or raise new questions in time. *See* Parks, *supra* note 313 at 93 ("The reduced-cues perspective may simply become a theoretic antique, given the continuing advances in network technology."). A full discussion of this topic is beyond the scope of this article.

458 MARSHALL MCLUHAN, UNDERSTANDING MEDIA: THE EXTENSIONS OF MAN 23 (2d ed. 1964).

459 It is unnecessary to go back to 1960, the reader's personal experiences may also support this point, consider seeing the same movie, on a large screen in a theater versus on a small screen television in a livingroom. Many readers will agree that these are vastly different experiences that may affect how they evaluate movies.

460 R. HARRISON, BEYOND WORDS: AN INTRODUCTION TO NONVERBAL COMMUNICATION 172-75 (1974); P. BOLLER, JR., PRESIDENTIAL CAMPAIGNS 298-99 (1984) ("Radio listeners had the impression that Nixon did as well as, if not better than, Kennedy in the confrontation; but televiewers, including Nixon's own fans, generally agreed that Kennedy came out ahead in the first debate."). *Cf.* M. CASSATA & T. SKILL, TELEVISION: A GUIDE TO THE LITERATURE 8 (1985) ("No one can deny, for instance, that in the televised 1960 presidential campaign debates, Nixon's haggard appearance, capped by a heavy growth of 'five o'clock shadow,' tipped the 1960 election scales in favor of the more alert, clean-cut Kennedy.").

tion.[461] A moment that was defined by the medium of television. Science and human experience dictate that the medium may define or create the message.

Initially in its *crudest* form, arbitration in cyberspace will consist of an e-mail exchange of copies of documents,[462] and responses to the arbitrator's or opposing party's questions. In essence, the arbitration will be an exchange of email. Based on this evidence, the arbitrator will make the award. Already, this process is too crude and fails to take complete advantage of the medium. Currently, real-time questioning of witnesses is possible using "chat" programs, and inexpensive real-time audio-video teleconferencing is increasingly available.

For the purposes of this discussion, the author assumes that the arbitration will be using a chat program to interrogate witnesses and to receive witness responses; the author further assumes that one or more witnesses's credibility is at issue. As Professor Berch noted the "transcription" of the testimony will result in

> some part of the communication [being] lost, because speakers use more than words to communicate: they rely upon a shared understanding of the metacommunicative frame in which the utterance is made. In addition to spoken words, this frame is indicated by paralinguistic features such as pitch, rhythm, and intonation, as well as visual features such as head nods, hand gestures and posture.[463]

Accordingly, up to 93% of witness communication may be lost by transcribing spoken words into ASCII symbols for transmission to the arbitrator.[464]

The law recognizes the importance of nonverbal communication. A fact-finder may consider the manner and demeanor of a witness in evaluating testimony.[465] As one appellate court found:

---

461 B. RUBIN, POLITICAL TELEVISION 18-20 (1967).

462 *Document* is being used in the broadest sense and includes both traditional paper documents and electronic documents such as e-mail or computer files.

463 Rebecca White Berch, *A Proposal to Amend Rule 30(B) of the Federal Rules of Civil Procedure: Cross-Disciplinary and Empirical Evidence Supporting Presumptive Use of Video to Record Depositions,* 59 FORDHAM L. REV. 347, 347 (1990) (footnotes and citations omitted). Professor Berch also found that lawyers prefer stenographic transcription of depositions to video depositions because stenographic transcription allows the attorney to shield the jury from unfavorable characteristics of the witness. *Id.* at 350.

464 *Id.* at 360 & n.67 (Ninety-three percent of all communication is non-verbal).

465 Cannon v. Cannon, 80 F. Supp. 79, 80 (D.D.C. 1936) ("Experience has demonstrated that one of the surest ways to determine the credibility of any witness is to observe the manner and demeanor of that witness on the stand."); EDWARD J. DEVITT, CHARLES B. BLACKMAR, MICHAEL A. WOLFF, FED. JURY PRAC. & INSTR. § 73.01 (1987).

> The judge before whom the cause was tried heard the testimony, observed the appearance and bearing of the witnesses and their manner of testifying, and was much better qualified to pass upon the credibility and weight of their testimony than this court can be. There are many comparatively trifling appearances and incidents, lights and shadows, which are not preserved in the record, which may well have affected the mind of the judge as well as the jury in forming opinions of the weight of the evidence, the character and credibility of the witnesses, and of the very right and justice of the case. These considerations cannot be ignored in determining whether the judge exercised a reasonable discretion or abused his discretion in granting or refusing a motion for a new trial.[466]

In Cyberian arbitration, there may only be words without a context before the arbitrator.[467]

The obvious response is televideo conferencing. But, these cues can also be affected by the technology, for example the placement of a camera. A truthful witness tends to face the questioner directly. If the camera is located on an angle to the questioner, and the witness looks at the camera while being questioned, the fact finder may misinterpret this as deceit.[468] And as at least one judge observed, "[i]n order to present even a normal appearance, most [people] must be made up or otherwise prepared" for the camera.[469] Moreover, in one study comparing radio, television, and newspaper, researchers discovered that radio listeners were able to detect deception 73.4% of the time, newspaper readers 64.2%, and television viewers 51.8%.[470] This study does not support televideoconferencing as the superior alternative. Another example, pauses and hesitations are associated with deceit; but in CMC, the pause or hesitation may be merely a communications lag caused by the technology and not the speaker. Computer Mediated Communications has a dramatic

---

466 Berch, *supra* note 463, at 401 n.76 (quoting Coppo v. Van Wieringen, 217 P.2d 294, 297 (1950) (quoting McLimans v. City of Lancaster, 15 N.W. 194, 195 (Wis. 1883)).

467 *See* Berch, *supra* note 463, at 362-71 (Professor Berch discusses in detail the importance of visual and paralinguistic communication in making credibility determinations.).

468 *Id.* at 364; Benjamin V. Madison III, Note, *Seeing Can Be Deceiving: Photographic Evidence in a Visual Age—How Much Weight Does it Deserve,* 25 WM. & MARY L. REV 705, 731-34 & n.177 (1984).

469 Hendricks v. Swenson, 456 F.2d 503, 508 (8th Cir. 1972)(Heaney, J. dissenting).

470 Richard Wiseman, *The Megalab Truth Test,* 373 NATURE 391 (Feb. 2, 1995). This study's methodology has been criticized. Oliver Braddick, *Distinguishing Truth from Lies,* 374 NATURE 315 (Mar. 23, 1995). Professor Wiseman's study is extremely interesting because it involved 41,471 subjects and attempted to move from laboratory research into the "real world."

impact on interpersonal and group dynamics. In asynchronous communication, the speaker experiences less stressful conversational demands so it is easier for the speaker to edit the response to adopt communication behaviors and disclosures that are more stereotypically desirable.[471] Another effect of CMC is that "removing the physical presence of others diminishes the influence a unanimous majority has on the opinion of an individual. The results further imply that in a CMC environment, subjects may be more critical and more willing to evaluate the information they are receiving."[472] Linguistic studies using mock jurors as subjects demonstrate that "[e]ven minor differences such as dialect, accent, voice quality, and linguistic fluency are related to how a listener views the speaker's trustworthiness, "likability," and benevolence."[473]

The effects of the interaction between the communications media and fact finding is especially problematic in the arbitral context.[474] Generally, arbitrators are free to ignore rules of evidence and other formalities.[475] Accordingly, unlike a judicial court which must affirmatively evaluate admissibility of evidence against the rules of evidence, arbitrators are free to let it all in and to sort it out, if they so desire, without formally weighing the impact of the media on the message.

The author is aware of the danger of extrapolating from a few linguistic studies in a laboratory setting to that of the cyberspace arbitral forum. But, these studies should at least cause individuals, involved in cyberspace fact-finding to consider if there are inherent limitations in the media and if so, how to best compensate for these limitations. Therefore, further studies of the fact finding and "judicial" decision making in CMC environments are needed.

---

471 Joseph B. Walther, *Impression Development in Computer-Mediated Interaction*, 57 W. J. OF COMM. 381, 394 (1993). The author assumes that these responses would also be more favorably received by the arbitrator.

472 Michael Smilowitz et al., *The Effects of Computer Mediated Communication on an Individual's Judgment: A Study Based on the Methods of Asch's Social Influence Experiment*, 4 COMPUTERS IN HUMAN BEHAVIOR 311, 319 (1988).

473 Charles M. Grabau and Llewellyn Joseph Gibbons, *Protecting the Rights of Linguistic Minorities: Challenges to Court Interpretation*, 30 NEW ENG. L. REV. 227, 314-15 (1996) (citation omitted).

474 Perhaps also in the cyberspace mediation context, "the opportunity to hear someone's voice or to look him or her in the eye changes how bargains are negotiated or whether any real bargaining occurs." Sara Kiesler et al., *Social Psychological Aspects of Computer-Mediated Communication*, 39 AM. PSY. 1123, 1132 (1984).

475 Bell Aerospace Co. v. Local 516, UAW, 500 F.2d 921, 923 (2d Cir. 1974). *See generally* Stephen H. Kupperman & George C. Freeman, III, *Selected Topics in Securities Arbitration: Rule 15c2-2, Fraud, Duress, Unconscionability, Waiver, Class Arbitration, Punitive Damages, Rights of Review, and Attorneys' Fees and Costs*, 65 TULANE L. REV 1547, 1580-81 (1991).

IX. CONCLUSION

Cyberspace is facing the challenge of becoming civilized and settled. The Wild West approach of community sanctions and shoot-'em-up flame wars no longer meets the needs of its inhabitants, but then neither does government regulation—the middle course, self-regulation best effectuates both the vision of the founders of cyberspace and the pragmatic needs of the real world. The original settlers have established a strong civil libertarian paradigm. Like the Old West, the "old cyberspace" had virtually unlimited resources and only a few individuals competing for access to those resources. This situation has now changed. The population is increasing at an almost exponential rate, and the demand for an increased bandwidth for new services is increasing even faster. In the future, there may not be enough room in cyberspace for each person to go out and do his or her own thing. Perhaps, someday in the future, Cyberians will have to sacrifice some freedoms. But that day is not yet here; currently, the cyberspace infrastructure is evolving apace with the social need for protection.

Technology provides individuals with effective, albeit not prefect, protection from the dangers of cyberspace. But even cyberspace technology is unable to protect people from themselves, so proper socialization is a prerequisite for effective technological solutions. For those dangers from which technology and individual initiative do not provide adequate protection, contract law or social enforcement mechanisms provide a sound basis for creating a "law" of cyberspace. As Oliver Wendell Holmes so aptly observed "[t]he life of the law has not been logic: it has been experience."[476] Given time, we may have sufficient experience with cyberspace to justify general legislation to govern it. Until then, first do no harm. So the core principles of the law of cyberspace should be based on the contract law model of private law making.

Cyberians will be surrendering substantial rights through contract to private government; therefore, the contracts must be intrinsically just (because there is a meeting of the minds) or extrinsically just (because the contract is fair). Hence, the current vogue of shrinkwrapping contracts in cyberspace must end. Contracting parties must take advantage of the technological options in cyberspace that reduce the transaction costs of negotiating contracts so that each contract represents the unique meeting of the minds — or at least a meeting of the electronic agents.

The unique transnational nature of cyberspace suggests that disputes in cyberspace should be resolved initially through arbitration. But because adjudication in cyberspace will be a creature of contract, Cyberians should knowingly consent to the jurisdiction of the "court" and the ap-

476 Oliver Wendell Holmes, Jr., 14 AM. L. REV. 233, 234 (1880) (book review).

pointment of the arbitrator. The arbitrator, while deriving power from the contract, should interpret each contract according to the contract principles of good faith and reasonableness. Additionally, the arbitrator should support core values that protect human dignity and personal freedom. Given time, these contracts and the decisions interpreting them may mature into a common law of cyberspace. Arbitration avoids difficult choice of law, forum, venue, and jurisdiction issues and may provide for "expertise" adjudication of disputes in areas where the adjudicator should be familiar with technology, customs, law, and be prepared to develop a law of cyberspace that is based on well-reasoned persuasive arbitral awards.

Finally, some acts in cyberspace have such a disproportionate impact in the real world outside of cyberspace that existing laws governing the real world should govern these acts. But for those crimes or torts, existing law is sufficient. In the end, there is simply no need for *sui generis* laws for cyberspace.

X. POST SCRIPT — *RENO v. AMERICAN CIVIL LIBERTIES UNION*[477]

Recently, the United States Supreme Court had the last word on the Communications Decency Act.[478] The Court affirmed the holding of two three-judge district court panels that provisions of the CDA violated the First Amendment to the United States Constitution.[479] The Court

---

477 1997 WL 348012 (U.S.). The court found provisions of the CDA unconstitutional in a 7-2 decision. The dissenting justices concurred that the "display," "indecency transmission," and "specific person provisions" as applied to more than one adult were unconstitutional. *Id.* at *27 (O'Connor, J., concurring in the judgment in part and dissenting in part).

478 Unless the proponents of the CDA unwisely return to Congress seeking CDA-II or Son-of-CDA.

479 *See* American Civil Liberties Union, 929 F. Supp. 824 (E.D. Pa. 1996), *aff'd* 1997 WL 348012; Shea on behalf of American Reporter v. Reno, 930 F. Supp. 916 (S.D.N.Y. 1996), *aff'd* 65 U.S.L.W. 3323 (1997).

rejected 47 U.S.C.A. § 223(a)(1)(B)(ii),[480] § 223(d)[481] (West Supp. 1997) as overbroad[482] without reaching the Fifth Amendment Due Process argument[483] or reaching the question of whether the unique characteristics of cyberspace prohibit any congressional legislation.[484]

A. SUMMARY OF THE COURT'S OPINION

The Court looked to the troika of cases upon which the United States' arguments rested: *Ginsberg v. New York*,[485] *FCC v. Pacifica Foundation*,[486] and *Renton v. Playtime Theatres*,[487] and rejected the government's contentions.[488]

---

480 Section 223(a) prohibits the knowing transmission of obscene or indecent messages to any recipient under 18 years of age. It provides that:

> (a) Whoever—
> (1) in interstate or foreign communications—
> * * *
> (B) by means of a telecommunications device knowingly—
> (i) makes, creates, or solicits, and
> (ii) initiates the transmission of,
> any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication;
> * * *
> (2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity,
> shall be fined under Title 18, or imprisoned not more than two years, or both.

481 Section 223(d), prohibits the knowing sending or displaying of patently offensive messages in a manner that is available to a person under 18 years of age. It provides that:

> (d) Whoever—
> (1) in interstate or foreign communications knowingly—
> (A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or
> (B) uses any interactive computer service to display in a manner available to a person under 18 years of age,
> any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; or
> (2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity, shall be fined under Title 18, or imprisoned not more than two years, or both.

482 1994 WL 328012, *14-*16.
483 *Id.* at *10, *14.
484 *Id.* at *10 n. 30.
485 390 U.S. 629 (1968).
486 438 US. 726 (1978).
487 475 U.S. 41 (1981).
488 1994 WL 328012,*10-*12.

1. *Ginsberg v. New York*

In *Ginsberg v. New York*, the Court rejected the defendants' broad reaching claim that freedom of expression cannot depend on whether a citizen is an adult or minor.[489] "In rejecting that contention [the Court] relied not only on the State's independent interest in the well-being of youth, but also [its] constant recognition of the principle that 'the parents' claim to authority in their own household to direct the rearing of children is basic in the structure of our society."[490] The Court distinguished the CDA from the New York State statute considered in *Ginsberg* on four grounds.

(1) The statute in *Ginsberg* did not bar parents from purchasing "indecent" materials for their children. In contrast, under the CDA neither the parents consent nor participation is a defense.

(2) The New York statute only applied to commercial transactions, and the CDA applies to all distribution of indecency whether commercial, not-for-profit, personal or social.

(3) The New York statute defined "indecency" as "utterly without redeeming social importance for minors" while the CDA fails to provide any definition of the term. And,

(4) The New York statute applied to persons under the age of 17 while the CDA adds an additional year by applying to persons under the age of 18.[491]

After distinguishing the CDA from the New York statute, the Court held that the statute in *Ginsberg* was substantially narrower than the CDA.

2. *FCC v. Pacifica Foundation*

In *FCC v. Pacifica*, the Court upheld a declaratory order of the Federal Communications Commission holding that recording of a comedic performance could be subject to administrative sanctions.[492] The FCC found that repetitive use of vulgar words referring to excretory, sexual activities or organs in the afternoon was patently offensive. In examining the regulation in the context of a pervasively regulated communications medium, the Court noted that "the First Amendment does not prohibit all government regulation that depends on the content of speech," so whether an indecent broadcast monologue is entitled to constitutional protection depends on the context of the broadcast.[493] "'[O]f all forms of communications broadcasting ha[s] received the most lim-

489 *Id.* at 10.
490 *Id.* at 11 & n.31.
491 *Id.* at *11.
492 *Id.*
493 *Id.*

ited First Amendment protection."[494] "[T]he Court concluded that the ease with which children may obtain access to broadcasts, 'coupled with the concerns recognized in *Ginsberg*,' justified special treatment of indecent broadcasting."[495]

The Court distinguished *Pacifica* on three grounds.

(1) Radio stations had been regulated for decades and the agency targeted a specific program to designate when—rather than if similar programs could be aired. "The CDA's broad categorical prohibitions are not limited to specific times [and] are not dependent on any evaluation by an agency familiar with the unique characteristics of the Internet."

(2) The FCC's order was not punitive while violation of the CDA subjects the violator to substantial criminal penalties.

(3) The FCC's order applied to an industry that had been historically regulated because warnings could not adequately protect the listener. In contrast, there is little chance of being accidently exposed to indecency in cyberspace, and there is no history of government regulation in cyberspace.

3. *Reton v. Playtime Theatres, Inc.*

In *Reton v. Playtime Theatres, Inc.*, the Court upheld a zoning ordinance designed to prevent crime and deteriorating property values — the secondary effects of adult theatres. The Court rejected the government's argument that the CDA was a cyberzoning ordinance. Unlike the statute in *Renton* which was aimed at the secondary effects of the adult movie industry, the CDA focuses on protecting minors from the primary effects of indecent speech.[496]

B. A NEW MEDIUM OF COMMUNICATION

After distinguishing the precedent cited by the United States, the Court then applied a medium specific analysis,[497] and found that unlike radio or television, the "democratic fora of the Internet [have never] been

---

494 *Id.* at *12.

495 *Id.* at *12 (quoting *Pacifica*, 438 U.S. at 749-50).

496 *Id.* at 12.

497 1997 WL 348012, *13 (citing Southeastern Promotions, Ltd. v. Conrad, 420 U.S. 546, 557 (1975)). Unfortunately, the Court did not adopt as a matter of general First Amendment jurisprudence that as communications industry develops new media such technology will presumptively enjoy a high level of protection. For example, Professor Tribe proposed a Twenty-Seventh Amendment:

> This Constitution's protections for the freedoms of speech, press, petition, and assembly, and its protection against unreasonable searches and seizures and the deprivation of life, liberty, or property without due process of law, shall be construed as fully applicable without regard to the technological method or medium through which information content is generated, stored, altered, transmitted, or controlled.

Tribe, *supra* note 42, at 39.

subject to the government supervision and regulation that has attended the broadcast industry."[498] The cyberspace is neither an invasive medium nor a scarce resource.[499] The court then concluded that there was "no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium."[500] Accordingly, cyberspace is entitled the highest level of First Amendment protection accorded to the traditional print media or the conversations of private citizens within their own homes.

C. OVERBREADTH ANALYSIS

The Court found that:

> the breadth of the CDA's coverage is wholly unprecedented. Unlike the regulations upheld in Ginsberg[501] and Pacifica,[502] the scope of the CDA is not limited to commercial speech or commercial organizations. *Its open-ended prohibitions embrace all nonprofit organizations and individuals posting indecent messages or displaying them on their own computers in the presence of minors.* The general unqualified term "indecent" and "patently offensive" cover large amounts of nonpornographic material with serious educational or other value.[503]

Moreover, the CDA subjected the violator to trial in the "community most likely to be offended by the message."[504] Yet, the CDA does not define "indecent" or "patently offensive as measured by contemporary standards, sexual or excretory activities or organs."[505] It is unclear how the two standards relate to each other. The vagueness of the CDA raises special First Amendment concerns. Such vagueness chills free speech, and because the CDA is a criminal statute, in addition to the stigma of a criminal conviction, its severe sanctions may cause speakers to remain

---

498 *Id.* (citation omitted). Because the appellees did not press the issue before the Court, the court declined the reach Judge Dalzell's observation that the characteristics of the Internet "lead to the conclusion that Congress may not regulate indecency on the Internet . . . ." *Id.* at *10 n.30 (quoting 929 F. Supp. at 877).

499 *Id.*

500 *Id.* at *14.

501 Ginsberg v. New York, 390 U.S. 629 (1968).

502 FCC v. Pacifica Foundation, 438 U.S. 726 (1978).

503 1997 WL 348012, *17 (emphasis added). The implication may be that the government can regulation commerical speech in cyberspace but not non-commerical speech of individuals or organizations.

504 *Id.*

505 *Id.* at 14.

silent rather than "communicate even arguably unlawful words, ideas, and images."[506]

The Court rejected the United States' contentions that the CDA is no more vague than the *Miller v. California* obscenity test.[507] The United States argued that "indecency" and "patently offensive" is the second prong of the *Miller* test. But the CDA lacks the key limiting provision "specifically defined by applicable state law," and in addition to applying to "sexual conduct," also applies to "excretory activities and sexual and excretory organs.[508] Further, the second prong's requirement that the work "lac[k] serious literary, artistic, political, or scientific value" allows the federal court to set a national floor for socially redeeming value.[509] The CDA contains no similar provisions. Because a more carefully drafted statute or less restrictive alternatives are possible, the Court concluded that the CDA imposed an unacceptable burden on adult speech.[510]

D. SOME CONCLUDING THOUGHTS

Perhaps, the Court's new use of the phrase "commercial speech" foreshadows a change in constitutional jurisprudence.[511] Traditionally, the Court used the term "commercial speech" to describe "advertisements" or other communications (speech) in conjunction with the sales of goods or services.[512] In cyberspace the commercial speech may also be commercial content. The two are not easily separable. In *American Civil Liberties Union,* the court used the term to refer to speech or content provided by commercial providers.[513] This poses the question,

---

506 *Id.*

507 (a) whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

Id. at 15 (quoting *Miller*, 413 U.S. at 24)(internal quotation marks and citations omitted in original).

508 1997 WL 348012, *15.

509 *Id.* at *15.

510 One such less restrictive alternative is the use of tagging or blocking software. See *id.* at 24-25 (O'Connor, J., concurring in the judgment in part and dissenting in part). Author's note: In cyberspace, the least restrictive test will almost always be met by a technological solution that focuses on the content receiver rather than the content provider. Only the content receiver is in a position to know what content is objectionable.

511 *Id.*

512 *See, e.g.*, Edenfield v. Fane, 507 U.S. 761 (1993); Central Hudson Gas & Electric Corp. v. Public Service Comm'n of N.Y., 447 U.S. 557 (1980); Pittsburgh Press Co. v. Pittsburgh Commission on Human Relations, 413 U.S. 376 (1973).

513 *See American Civil Liberties Union*, 1997 WL 348012, *7 n.23 (distinguishing between commercial and non-commercial content providers). *10-*12 (distinguishing *Ginsberg* because it applied only to commercial content providers); *13 (distinguishing *Sable* because it

whether the Court for reasons of style or through inadvertence used a technical term in the colloquial sense or whether the Court signaled a change in constitutional jurisprudence. The strongest argument against the Court expanding the definition of "commercial speech" is that the dissenting opinion did not remark upon it. The strongest argument for the expanded definition is the repeated new use of "commercial speech" in the context of the first United States Supreme Court opinion by an experienced justice considering cyberspace, a new and novel communications medium, strongly suggests that the Court has added a new wrinkle to the term "commercial speech." Justice Stevens has authored six commercial speech opinions for the Court, one in each of the last two terms.[514] This suggests that Justice Stevens is aware of the parameters of the phrase "commercial speech" used in its traditional sense.

The Court in *American Civil Liberties Union* is making that common sense distinction between speech made by individuals or not-for-profit groups and commercial organizations. Although, the use of the term "commercial speech" in this context appears novel, the Court has drawn this distinction between text and metatext before. The difference is between speech that exists to vindicate constitutional rights and speech that is for pecuniary gain. The classic example of this involves attorney solicitation cases. The Court has uniformly held that an attorney soliciting a (potential) client in order to litigate for a not-for-profit entity that exists for the purpose of vindicating constitutional rights is protected speech.[515] Yet, the Court has upheld such statutes when the attorney was motivated by pecuniary interests.[516] Similarly in cyberspace, the court

---

applied to commercial telephone communications); *15 (distinguishing *Miller* because it applied to commercial vendors); *17 (distinguishing "the regulations upheld in *Ginsberg* and *Pacifica*, [because] the scope of the CDA is not limited to commercial speech or commercial entities."); and *19 (distinguishing between commercial and noncommercial speakers).

514 *See, e.g.*, Dan Glickman, Secretary of Agriculture v. Wileman Brothers & Elliott, Inc., 1997 WL 345357, 65 USLW 4597 (1997); Liquormart, Inc. v. Rhode Island, 116 S.Ct. 44 (1996); City of Cincinnati v. Discovery Network, Inc., 507 U.S. 410 (1993); Peel v. Attorney Registration and Disciplinary Com'n of Illinois, 496 U.S. 91 (1990); FW/PBS, Inc. v. City of Dallas, 493 U.S. 215 (1990); Lowe v. S.E.C., 472 U.S. 181 (1985).

515 Where political expression or association is at issue, this Court has not tolerated the degree of imprecision that often characterizes government regulation of the conduct of commercial affairs. The approach we adopt today in *Ohralik*, 436 U.S. 447, that the State may proscribe in-person solicitation for pecuniary gain under circumstances likely to result in adverse consequences, cannot be applied to appellant's activity on behalf of the ACLU. Although a showing of potential danger may suffice in the former context, appellant may not be disciplined unless her activity in fact involved the type of misconduct at which South Carolina's broad prohibition is said to be directed.

In re Edna Smith Primus, 436 U.S. 412, 434-35 (1978); National Association for the Advancement of Colored People v. Button, 371 U.S. 415, 428-29 (1963). .

516 *See* Ohralik v. Ohio State Bar Association, 436 U.S. 447, 457 (1978) ("In-person solicitation by a lawyer of remunerative employment is a business transaction in which speech is an essential but subordinate component. While this does not remove the speech from the

may wish to be especially solicitous of speech made for individual, not-for-profit, or educational purposes in the absence of pecuniary motives versus speech that exists as commercial content for sale.

The truism of cyberspace is that everyone is potentially a content provider and consumer and in many ways access to cyberspace is equal for all.[517] Yet, it does not necessarily follow that the law must impose the same liabilities and duty on all content providers. While it *may* be reasonable to force commercial providers "to cope with the community standards of every hamlet into which their goods may wander,"[518] it would not be reasonable to ask each individual to anticipate the community mores of every geographic location from which some person could access content and to be prepared to defend that speech in every hamlet.[519] Accordingly, the Court may be preparing to recognize in cyberspace the existing realities of speech in the real world.

protection of the First Amendment, . . . it lowers the level of appropriate judicial scrutiny."). It is important to note that *Primus* and *Ohralik* were handed down together. 436 U.S. at 422.

517 *Cf.* Hardy, *supra* note 140, at 1041.

518 Hamling v. United States, 418 U.S. 87, 144 (1974) (Brennan, J., dissenting).

519 Randolph Stuart Sergent, *The Hamlet Fallacy: Computer Networks and Geographic Roots of Obscenity Regulation*, 23 HASTINGS CONST. L.Q. 671 (1996).