Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces

Anne Wells Branscomb

Follow this and additional works at: http://digitalcommons.law.yale.edu/ylj

Recommended Citation
Available at: http://digitalcommons.law.yale.edu/ylj/vol104/iss7/5

This Article is brought to you for free and open access by Yale Law School Legal Scholarship Repository. It has been accepted for inclusion in Yale Law Journal by an authorized editor of Yale Law School Legal Scholarship Repository. For more information, please contact julian.aiken@yale.edu.
Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces

Anne Wells Branscomb†

I. INTRODUCTION

Principles underlying the First Amendment favor an information agora promoting and embodying democratic ideals. The pioneers of what is often called cyberspace, the electronic environment through which the computer literati engage interactively, anticipate that this new frontier promises the opportunity for full participation in the electoral process as well as development of a flourishing computer-mediated information marketplace. The experiences of these computer-competent citizens (sometimes called “netizens”) using the Internet, a backbone for interconnecting computer-

† Research Associate, Project on Information Resources Policy, Harvard University <branscom@csn.org>; Scholar-in-Residence, Annenberg Public Policy Center, University of Pennsylvania (1994–95). The author wishes to acknowledge the contributions to her analysis of her colleagues in three computer-mediated conferences: Cyberia and NEWJURIS on the Internet and The Law of the Electronic Road on LEXIS Counsel Connect.

1. Agora comes from the Greek, and describes a large central open square in the city where merchants brought their wares and where citizens came to exchange ideas, a community gathering place where all manner of political, economic, and social transactions were consummated. See MERRIAM WEBSTER’S COLLEGIATE DICTIONARY 24 (10th ed. 1993).

2. See Turner Broadcasting Sys., Inc. v. FCC, 114 S. Ct. 2445, 2470 (1994) (“Assuring that the public has access to a multiplicity of information sources is a governmental purpose of the highest order, for it promotes values central to the First Amendment.”); Associated Press v. United States, 326 U S. 1, 20 (1944) (“The widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public. . . .”)

3. The term “cyberspace” was introduced in 1984 by William Gibson, in his novel Neuromancer, to describe the virtual space in which his characters interacted. WILLIAM GIBSON, NEUROMANCER 51 (1984). It has been adopted by users of electronic networks more broadly to encompass the entire experience of communicating through computer-mediated networks, both in the futuristic view of a three-dimensional electronic representation of the real world and also to include all manner of interactivity via text only.

4. The term “netizens” is borrowed from the recent works of two authors. See Jim McClellan, Cyberspace: Judge Dread, OBSERVER (London), Jan. 29, 1995, at 76; Howard Rheingold, “Web” Spreads into a Wildfire, DENVER POST, Jan. 13, 1995, at 22.

5. One commentator has described the Internet as follows: The Internet is best thought of as a suite of digital communications—packet-switching protocols that, when adopted by many nonhomogeneous digital networks, create the equivalent of a virtual, interactive overlay network. The Internet is not a physical network. It has no owner, no control point, sells no services. Thus the Internet is better thought of not as a network, but as a remarkably powerful array of internetworking capabilities, through which great numbers of
mediated communications globally, suggest that we now have within our grasp a technology designed to bring together like-minded individuals, regardless of where they live, work, or play, to engage in the creation of a new type of democratic community: a community unbounded by geographical, temporal, or other physical barriers.

These new experiments in democracy do not simply represent a futuristic vision. On the contrary, they pervade the electronic environment. Observers of online activity have recognized inclinations to preserve individual and group autonomy without governmental intrusion or authoritarian censorship. These inclinations are fully in accord with the motivations that brought the early pioneers to the new continent to preserve their religious independence, develop new frontiers, and exert self-determination in their systems of governance. Many of these new experiments have led to the development of user groups that look upon themselves as "virtual communities" entitled to deal with problems arising in the electronic environment as they find appropriate. Such virtual communities can be said to occupy separate and diverse cyberspaces, essentially carving out domains of their own over which they choose to exert jurisdiction. Therefore, the generic term "cyberspace" does not aptly describe these evolving communities. For the purpose of this Essay, I shall refer to the varying electronic domains as cyberspaces and refer to the whole as the "Networld."  

The unique quality of being able to post messages to and from everyone with an electronic address without editorial control or the intervention of elected representatives promises to become one of the most powerful democratic tools ever devised. Because these cyberspaces in the Networld ignore space, time, and physical circumstances, they remove the visual cues that often inhibit or facilitate communication. Furthermore, the marvels of digital communication have erased many of the prejudices that arise from these culturally specific visual cues. Therefore, the encounter becomes a true meeting of the minds, where the power of persuasion resides in what is said—that which is protected from governmental interference by the First Amendment—rather than what is seen.

users can reach one another and a great array of sources of information around the world through the facilities of many networks.

Conversation with Lewis M. Branscomb, Professor of Science and Technology Policy, John F. Kennedy School of Government, Harvard University, former Chief Scientist of IBM and Director of the John F. Kennedy School of Government Project on the National Information Infrastructure (Feb. 1995).

6. According to Linda M. Harasim, "Human communication has become the major use of computer networks and has transformed them into a social space where people connect with one another. Computer networks are not merely tools whereby we network; they have come to be experienced as places where we network: a networld." Linda M. Harasim, Networlds: Networks as Social Space, in GLOBAL NETWORKS: COMPUTERS AND INTERNATIONAL COMMUNICATION 15, 15 (L.M. Harasim ed., 1993); see also NEAL STEPHENSON, SNOW CRASH 18 (1992) (referring to this new phenomenon as the "Metaverse"). Other metaphors are equally applicable: information superhighways, global infobahn, i-ways, electronic cafés, information marketplaces, electronic playgrounds.
In this Essay, I examine some of the ways in which cultural behavior developing in cyberspaces is challenging the First Amendment. In addition, I explore the manner in which intrusion by real-world communities may inhibit the free flow of information in cybercommunities and threaten not only the independence of such communities but also the value of electronic communication as a vehicle for democratic discourse. Given the development of new cybercommunities seeking to engage in self-governance, there is a very real possibility that the nation-state as a mediator or determinant of socially and legally acceptable behavior may be displaced by smaller “virtual communities” online that create their own behavioral norms. If so, then the First Amendment may have little effect on the practices and procedures employed within the Networld.

"Netizens," however, do assert what they call a First Amendment right of unencumbered access to whatever information they deem personally useful or desirable, and deplore intervention by outsiders or even the proscriptions of their own institutions. Although it is not accurate to describe this claim as a First Amendment right, clearly many Internet users’ developing expectation of freely flowing channels of information without censorship by outsiders cannot be ignored. Many of the users of the commercial information services share this expectation. Thus, there is no reason why something akin to the First Amendment may not be asserted vis-à-vis transport providers offering services in autonomous domains.

In order to examine the conflicts and questions that the First Amendment will provoke in cyberspaces, I focus upon three areas of controversy: anonymity, autonomy, and accountability. These three subjects represent interlocking and competing forces. The elevation of one of these forces has important implications for the other two. For example, a right of absolute anonymity may foreclose accountability, whereas full accountability of users may mean the prohibition of anonymity. Similarly, full autonomy and control over the flow of information may isolate one from access to information upon which democratic discourse and a healthy exercise of the functions of self-governance in a democratic society depend. Therefore, it is necessary to explore how these forces interact in the context of actual cyberconflicts. In order to ensure that we are exploring these forces with a common understanding, I briefly define the forces of anonymity, autonomy, and accountability in the following Sections.

A. Anonymity

True anonymity in the Networld would mean that no one could trace the source of an electronic message. The First Amendment prevents the outlawing of true anonymity, although it only prevents governmental interference with anonymous messages. For this reason, the new cybercommunities as well as
commercial providers of electronic environments must grapple with the propriety of anonymity. The possibility of genuine anonymity implicates both the positive value in protecting the sources of certain information as well as the danger inherent in allowing individuals to speak and write without detection. For some computer users, anonymity is merely fun and games. For other anonymous posters, however, the ability to remain unknown removes many of the layers of civilized behavior as they realize that they can escape responsibility for negligent or abusive postings.

There are numerous situations in which anonymity seems entirely appropriate and even desirable. Psychologists and sociologists point out that people benefit from being able to assume different personae. It is therefore natural that individuals use electronic communication to disguise themselves, as in costume balls in the multiuser dungeons (MUDs) that Howard Rheingold describes. As one student admitted, “It’s my hallucinogen of choice. . . . I love being able to slip into another body, another persona, another world.”

There are many other valid justifications for preserving a limited right to anonymity. The media often cite “a prominent source” who does not wish to be identified, and pseudonymous authors have long been with us, sometimes in the past to prevent disclosure that the writer was female for fear her work would not be published were her gender known. Usually, in these cases, the publisher or journalist knows the source and vouches for its integrity. Anonymity has also been protected in cases in which actual retaliation or harm may ensue if the source of the writing is known, as in the case of whistle-blowers or political dissidents under authoritarian regimes.

Yet, there are also many valid reasons supporting prohibition of anonymity. Disguising the sources of messages or postings relieves their authors from responsibility for any harm that may ensue. This often encourages outrageous behavior without any opportunity for recourse to the law for redress.

7. Sarah Kiesler, Professor of Sociology at Carnegie Mellon University, Address at the Workshop on Rights and Responsibilities of Participants in Networked Communities, in Washington, D.C. (Nov. 6, 1992).
8. Howard Rheingold, The Virtual Community 145–50 (1993). MUDs are multiuser dungeons or multiuser dimensions, a technology created by the software in a computer to provide imaginary landscapes in which participants may create their own “virtual” reality worlds through the use of word descriptions. Players join in a group activity, collectively building a communal space in which to conduct their games. There are also serious professional uses of such electronic environments in which workgroups use the MUD to conduct cooperative research, build analytical models, and exchange views on the state of the art in their respective fields.
of grievances. Law enforcement officials or lawyers seeking to file a civil suit might not be able to identify an individual to hold responsible.10

Many providers of computer-mediated facilities do not permit genuine anonymity. They keep records of the real identity of pseudonymous traffic so that abusers can be identified and reprimanded.11 Recent years, however, have witnessed the development of a trend towards the establishment of “anonymous remailers” who provide a guarantee that messages cannot be traced back to their sources; diverting traffic through several of these remailers can effectively render an audit trail impossible, once again raising the specter of true anonymity.12

10. Drivers on the real highways are not permitted access without a motor vehicle license so, logically, it should be possible to require users of networks to be responsible and identifiable. Indeed, Professor Arthur R. Miller has made this argument quite persuasively with respect to the deployment of anonymous telephone calls:

I believe that anonymity—not privacy—is what is being sought by a telephone caller who objects to having the telephone number revealed by Caller ID. The question then is whether a person has a right to hide behind a veil of anonymity in making a telephone call over the public telephone network . . . . Society, for example, requires that automobiles have license plates to travel on a public road. This modest deprivation of anonymity is designed to promote accountability. Those who insist on anonymity in placing telephone calls are, in essence, saying they do not want to be accountable on the communications network, which is quite analogous to driving without a license plate. See Hearing on S. 2030 Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary, 101st Cong., 2d Sess. 265 (1990). Real highways, however, do not carry the same First Amendment vulnerabilities that electronic superhighways do.

11. Harvard University forbids its students from posting anonymous messages. See HARVARD ARTS & SCIENCES COMPUTER SERVS., HARVARD UNIVERSITY, COMPUTER RULES AND ETIQUETTE: STUDENT COMPUTING AT HARVARD 3 (Dec. 1993). A real controversy has arisen over whether Harvard students may post such messages in non-Harvard electronic spaces that permit or even encourage anonymous posting. The University of North Carolina permits lurkers to remain unidentified but forbids and technically blocks uploading of messages until a user has a verifiable account and user identification on the system. Interview with Paul Jones, Internet Information Specialist, Office of Information, University of North Carolina, in Chapel Hill, N.C. (Apr. 1993).

Other universities do not have strict enforcement policies. For example, MIT has no specific policy but attempts to discourage anonymous postings while recognizing the difficulty in excluding them altogether. E-mail from James D. Bruce, Director of Computing, MIT, to author (Mar. 9, 1995) (on file with author). Moreover, some universities do not have unitary policies governing the computer uses of all of their students. For example, some schools within the University of Pennsylvania prohibit anonymous messages while others do not. Interview with Dan Updegrove, Assistant Director of Computing Services, University of Pennsylvania, in Philadelphia, Pa. (Feb. 2, 1995). In any event, the practice of offering pooled computer facilities in dormitories and various schools means that students using such pooled resources are not identified. Id. With such a pooled system, it would be possible to use audit trails to track abusive messages to particular computing stations. To trace a message to a particular individual, however, would require knowing that a station was used only by one person or would require that a supervisor record both the names of students entering a computing facility and which computers they used during a session.

Commercial information providers are also devising ways to deal with the difficult question of appropriate levels of anonymity. For example, America Online permits the use of pseudonyms and makes no effort to prescreen messages but reserves the right to curtail service to members who abuse the privilege by posting abusive anonymous messages. Letter from David W. Phillips, Assistant General Counsel, America Online, Inc., to author (Mar. 14, 1995) (on file with author).

12. See, e.g., Steven Levy, How To Launder Your E-mail, WIRED, June 1994, at 50, 50–51; Joshua Quittner, An Interview with Johan Helsingius, WIRED, June 1994, at 50, 52–53.
B. Autonomy

Autonomy means the right to exert some modicum of control over one's electronic environment. Efforts to devise some rules to preserve autonomy must include consideration of several challenging questions. First, is there a right to prevent access to, or control the timing and terms of disclosure of, information about oneself, one's corporation, or one's institutional entity? Second, may certain cyberspaces be maintained as private spaces in which the users themselves determine the governing rules? Third, how can one ensure the confidentiality of messages posted to trusted colleagues? Such issues of autonomy over communications present difficult challenges in the cyberspaces.

These questions are often clustered within the area of law called privacy. Privacy law is a fairly recent arrival on the horizon, but it, too, derives at least some of its virtues from First Amendment principles. At a minimum, privacy can be translated into some sanctuary to which one may retreat—a personal space and the ability to screen out unwanted or offensive messages. Although there may be a First Amendment right to speak, there is no comparable right to be heard.13 Furthermore, privacy must mean some degree of autonomy over personal information and how it is obtained and deployed by others, including governmental entities that may have a compelling interest in obtaining the information.14

Control over personal information may appear to be the flip side of freedom of speech, that is, the freedom not to speak. This freedom not to speak simply protects the right not to have information disclosed without consent or in a manner that may be contrary to one's interests. This has become a matter of considerable concern; the opportunities for unwitting disclosure in cyberspaces range from uses of electronic identification for access to the system, to uses of credit cards for purchases, identification of viewer preferences, communication of medical records, and countless ways in which computerized identification is coupled with personal preferences and behavior. Americans have very little comprehension of or agreement about what privacy entails, but 84% are concerned about it, and 78% feel that they have lost control over personal information about themselves.15 The confusion about privacy indicated by these statistics is compounded in the Networld.

14. Clearly, governmental interests would be adversely affected if birth and death records, motor vehicle registrations, voting identification, and property ownership records were not available for public processing and recordation.
C. Accountability

Accountability refers to the acceptance of responsibility for one's actions. Without accountability, there is no basis upon which an injured party can initiate a tort action to redress grievances. Technically, the law would hold the initiator of a defamatory message accountable for any deleterious consequences associated with it. If one cannot hold the poster of an abusive message responsible, because it is anonymous or the poster is judgment-proof, the defendant must be the provider of the electronic space containing the message. Potential litigants and their legal counsel have not hesitated to seek the source of the deepest pockets.\textsuperscript{16}

The complexity of the relationships between anonymity, autonomy, and accountability is most apparent when attention is focused upon accountability. For example, anonymity or pseudonymity on the electronic highways is rampant and seems to strip users of the civility that the face-to-face encounter has engendered in most modern societies.\textsuperscript{17} It also facilitates the distribution of false information that may have detrimental consequences.\textsuperscript{18} Although the users of anonymous messages seem adamant in claiming an absolute right to their anonymity,\textsuperscript{19} this anonymity prevents the legal system from holding them accountable for abuses of the privilege.

This lack of accountability throws the legal responsibility back upon the providers of the cyberspaces and transforms them into censors, a role none of them wishes to play. Being required to monitor all digital traffic would place an undue burden upon these information providers, all of which are still in their infancy. This would be especially true for the smaller bulletin board operators (sysops), who are, for the most part, judgment-proof. There is as yet no consensus regarding where to place the burden for behavior that contravenes well-established legal restrictions.

\textsuperscript{16} One difficulty is that many of the abusers have been young users just learning their computer skills, who have little or no financial capability to pay damages imposed by a legal judgment.

\textsuperscript{17} See Lee Sproull & Sara Kiesler, Computers, Networks, and Work, in SOCIAL ISSUES IN COMPUTING: PUTTING COMPUTING IN ITS PLACE 335, 338–39 (Chuck Huff & Thomas Finholt eds., 1994).

\textsuperscript{18} Marian Burros, Eating Well, N.Y. TIMES, Feb. 1, 1995, at C3 (discussing potential problems created by false and misleading electronic information regarding health and nutrition).

\textsuperscript{19} Walter S. Mossberg, Accountability Key to Democracy in On-line World, PLAIN DEALER (Cleveland), Feb. 5, 1995, at 4G. Anonymity is a cherished tradition among some on-line veterans, who enjoy the fantasy aspect of these communities and argue that it enables shy or socially outcast people to finally blossom via modem. . . . It sure makes it easier to spread wild conspiracy theories, smear people, conduct financial scams or victimize others sexually.

\textit{Id.}
D. *Is There a Place for the First Amendment in Cyberspaces?*

The three issues I have chosen to explore, the assertion of a right to true anonymity, claims to autonomy over the information transmitted online, and questions of accountability for misuse or abuse of the information resources, are traditional sources of controversy in First Amendment history. Such issues are continually implicated in the debates and conflicts arising out of online activity. The current First Amendment-type controversies arising in both actual encounters in cyberspaces and hypothetical discussions are useful tools for exploring what may occur as computer-mediated communication becomes more widely available throughout the world. The Internet, as well as publicly available information service providers such as CompuServe, Prodigy, America Online, GEnie, Delphi, ImagINation, and the WELL, present prototypes of the kinds of information marketplaces that are possible and also demonstrate the kinds of abuses and dilemmas that can occur and challenge First Amendment principles.

While exploring the capabilities of interactive computer-mediated dialogue and the First Amendment conflicts arising as by-products of such communication, it must be understood that the First Amendment is a local ordinance. Many, indeed, most other countries, do not have the equivalent of a constitutional prohibition against interference with freedom of speech. Still, the right to freedom of speech remains a sacred tradition in United States media law and has correlative rights in the laws of other Western cultures, the United Nations Universal Declaration of Human Rights, as well as seeds that have been sown in the constitutions of other countries. The inhabitants of cyberspaces often treat the First Amendment as a given statement of protection in their world, which insulates them not just from interference from the U.S. government but from all intrusions or confrontations with the real world.

In the pioneering days of what has become the Internet, users and their usages were largely ignored. The cyberspaces were used primarily for professional and academic purposes, subject only to the “acceptable use policy” (AUP) mandating that the network services be used for the research community and its scientific goals. Some commercial information service providers write contracts describing their expectations of appropriate behavior and reserving the right to withdraw services from those who do not comply.

As more and more computer users arrive in these cyberspaces, they bring expectations that the legal norms of the real world will apply. Lawyers, judges, and juries, often without any genuine understanding of or experience with

---

20. See ELECTRONIC FRONTIER FOUND., EFF'S GUIDE TO THE INTERNET § 4.6 (version 2.2 1994).
22. See infra note 65.
23. See, e.g., America Online Terms of Service (TOS) § 4.2, available online at America Online, Members' Online Support Area, Member Services.
electronic networks, are asked to prosecute, defend, or decide controversies arising within the cybercommunities. Thus, more and more often, confrontations are arising between the legal expectations of the real world and the developing "netiquette" of the "netizens" of cyberspaces. Whether "netizens" may assert a cyberjurisdiction to govern their electronic behavior, a jurisdiction that is separate from and perhaps independent of the legal norms of the real world, is questionable. Without such grants of jurisdictional authority, however, transferring legal norms from the real world may result in the application of rigid rules inappropriate to the cybercommunities and may jeopardize the full development of the information agora that the technology promises.

II. AREAS OF CONfrontATION

In order to explore these First Amendment issues, I turn to a discussion of some actual confrontations that have arisen in cyberspaces in recent months. In some of the cases, traditional solutions to First Amendment problems have been efficacious in solving problems in the Networld; in others, quite troublesome. The critical question is whether "new wine can be poured successfully into an old bottle," or whether new legal norms must be devised for the governance of the Networld. For the purposes of analysis, I divide the cases into several categories: those in which existing laws have been applied somewhat successfully to the cyberspaces, those in which "netizens" have taken governance into their own hands and devised their own means of dealing with what they perceive to be abuses, those in which cybercitizens are...
at odds with the legalities of the local jurisdiction, and those for which no legally enforceable standard of care yet exists.

A. Transfer of Existing Rules of the Real Community into the Cybercommunity

The first case I will explore is one in which existing law was applied quite effectively to a controversy arising online. Moreover, the solution met with the satisfaction of the defendant commercial information provider. Significantly, this case involved an archetypal First Amendment conflict: a claim of defamation. The new and challenging twist was that the alleged defamatory material appeared in an online bulletin board rather than in a newspaper or on a public broadcast. Despite the new form of media, the fundamental questions did not change. The court could rely on existing defamation cases as it attempted to apply the legal standards to the facts at issue. Indeed, the very nature of this controversy may have made it ripe for easy importation of existing legal norms, unlike some of the other controversies that involve fact patterns unique to the new media.

Few cases have been definitive in determining to what extent commercial information providers and sysops must monitor, or are prohibited from monitoring, electronic traffic. If the traffic constitutes public e-mail, the Electronic Communications Privacy Act (ECPA)\(^{26}\) would forbid monitoring. If the provider is considered to be the publisher, however, it would be held to standards of editorial control and would be accountable in law to those defamed within its services.

In 1991, activity on the CompuServe system generated a case with significant implications for these issues, \textit{Cubby, Inc. v. CompuServe Inc.}\(^{27}\) The plaintiff sued CompuServe for defamation because of objectionable material posted within an electronic segment called Rumorville USA. This was one component of the Journalism Forum, a daily newsletter operated by Don Fitzpatrick Associates of San Francisco.\(^{28}\) CompuServe claimed to have neither knowledge of the alleged defamatory material nor the opportunity to exert control over it. Furthermore, Don Fitzpatrick Associates had signed a contract with CompuServe whereby the former “accept[ed] total responsibility for the contents” of material that it edited.\(^{29}\) As a consequence, Don Fitzpatrick Associates constituted a responsible party that could have been held liable by the alleged defamed party, but the litigant chose CompuServe, which was more likely to be financially solvent.

\(^{28}\) \textit{Id.} at 137.
\(^{29}\) \textit{Id.}
The court found that CompuServe was only a distributor of Rumorville USA, and, as such, was not required to be aware of everything contained in its electronic memory.\textsuperscript{30} The court was quite explicit in its absolution of CompuServe:

CompuServe has no more editorial control over such a publication than does a public library, book store, or newsstand, and it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so. . . .

Technology is rapidly transforming the information industry. A computerized database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor such as CompuServe, than that which is applied to a public library, book store, or newsstand would impose an undue burden on the free flow of information.\textsuperscript{31}

Although the decision was welcomed by sysops and commercial information providers alike, it should not be accepted as the final word on the subject. Not only was this a district court case, but it involved an information provider that had undertaken full responsibility pursuant to its contract with the manager of the particular cyberspace service. This is quite different from other information providers who may, like America Online, have partnership agreements with their providers or who may, like Prodigy, adopt the role of publisher and assume responsibility for monitoring some of the forums. Nor does the case begin to address the volatile and diverse universe of bulletin board sysops, ranging from small-time personal operators that look more like personal mailboxes to very large commercial operations providing access to whole archives of graphic images.

The \textit{Cubby} case merely holds that commercial providers who make no effort to monitor content and serve primarily as information distributors may be relieved of liability for the content of messages within their systems. The case offers no solace to the thousands of individual bulletin board operators nor to the volunteer newsgroup moderators on the Internet, who, because they assume responsibility for screening messages, may be held legally responsible to nonparticipating users allegedly defamed or damaged by electronic conversations taking place within the computer-mediated environment.

\textit{Cubby} is likely to be only the first foray into the deliberation necessary to determine how to assign liability and accountability for message streams that may differ markedly, even when provided by the same entity. Confrontations between providers of these networked worlds and those who feel abused by the

\textsuperscript{30} \textit{Id.} at 140.

\textsuperscript{31} \textit{Id.}
words passing through them in digital form are likely to be troubling and expensive, unless alternatives can be devised to handle these situations satisfactorily.32

B. Unsuccessful Translation of Real-World Legal Rules

A recent controversy regarding online activity demonstrates the difficulties confronting information providers as they attempt to accommodate their electronic services to the expectations of users. The incident reveals some deep misunderstandings among subscribers concerning the differences between public and private electronic spaces and highlights the inherent problems in dealing with a highly differentiated set of cyberspaces that range from electronic mail to public forums to electronic shopping malls.

Prodigy, as a joint venture between Sears and IBM, offers an environmentally neutral safe haven for Middle American families seeking an electronic home as comfortable as Disneyland.33 Prodigy has been the subject of numerous attacks on its policies by subscribers,34 but the one examined here involved hate messages from a subscriber that had been originally transmitted to many subscribers within the protected e-mail service. One of those most offended by the message sought to have it posted in a public space so that other subscribers could come to know both its subject and source. Prodigy, by its own account, reviewed and rejected the recommendation to post this message in public spaces fifteen times because posting it would be disturbing to Prodigy subscribers and "'grossly repugnant to society's standards of decency.'"35 These messages fell into the category of "'blatant expressions

32. See, for example, the case recently filed by an investment firm, Stratton Oakmont of Lake Success, New York, against Prodigy and subscriber David Lusby of Key West, Florida. The suit seeks $100 million in actual damages and an additional $100 million in punitive damages. Peter H. Lewis, Libel Suit Against Prodigy Tests On-Line Speech Limits, N.Y. TIMES, Nov. 16, 1994, at D1. The offending message appeared in the Money Talk discussion group, where a warning by Prodigy notifies the viewer that "Prodigy does not verify, endorse or otherwise vouch for the contents of any note and cannot be held responsible in any way for information contained in any such note." Id. at D2. Nonetheless, the message directly accused the plaintiff firm of illegal activity in the context of its participation in an initial public offering, exclaiming: "This is fraud, fraud, fraud and criminal!!!!!!!" Id. The individual defendant, a former employee of Prodigy, had not used his account for "some time" and denies responsibility for the message. Id. Prodigy agreed in court to block messages concerning the complainant for three months, "to track down" the offending party, and "to provide the court with a detailed explanation of how messages to the system are posted, screened and monitored." Id.


34. Several of these incidents are discussed extensively in ANNE W. BRANSCOMB, WHO OWNS INFORMATION? FROM PRIVACY TO PUBLIC ACCESS 98–103 (1994).

35. Prodigy Did Not Publish, supra note 33 (quoting Henry Heilbrunn, Senior Vice President of Prodigy).
of bigotry, racism and hate'' that would no longer be posted in public spaces. Prodigy managers were quite clear, however, that they did not intend to become “thought police,” and they permitted posting of some of the less repugnant messages.

This incident came to the attention of the national media when the Anti-Defamation League accused Prodigy of anti-Semitism, and the entire episode created a great furor over appropriate behavior in the Networld. The most offending message actually received a great deal more media attention through republication than it ever would have received had the national media not picked up the story.

Prodigy claimed that it attempts to ensure that messages posted in public spaces will not offend its subscribers. Prodigy sources also claimed, however, that monitoring e-mail was forbidden, although it was technically possible, as it is for most message providers, to screen the message traffic. If Prodigy is in the position of a publisher, in present legal terms, it was well within its rights to assert editorial control over whatever electronic message traffic appeared in public spaces. As a transmitter of electronic mail services, however, it would be beholden to the legal restriction that such mail not be monitored. Eventually the media attack subsided with apologies on all sides and a recognition that, at least under current law, Prodigy was within its rights in exercising editorial control over messages posted in public spaces while attempting to exert as light an editorial pencil as possible in the interest of providing an open forum for the discussion of public issues.

In this case, existing rules were eventually applied to protect the publisher from legal liability but not from public approbation for what some considered reprehensible behavior. There is, however, a difficulty in applying existing legal metaphors to a Networld in which an information provider may logically seem to fall under the ambit of several legal regimes. On some channels offered by Prodigy, the information provider is acting in the normal manner

36. Id. (quoting Ted Papes).
37. See John Buskin, Will Free Speech Byte the Dust?, NEWSDAY, Oct. 30, 1991, at 84 (“Prodigy also made it clear that it was not prepared to play bulletin-board thought police.”).
38. See Jerry Walker, Swift PR Action Chills Anti-Semitism Charges, SPORTING NEWS, Dec. 1991, at 36 (“At first, ADL’s complaint got limited pickup and for the most part, the reports were neutral. But on the morning of October 23, the situation changed when New York Newsday, which has a large Jewish readership in the New York Area, published a page one story, headlined ‘High-Tech Hate.’”). The actual messages read: “Hitler had some valid points too,” “Remove the Jews and we will go a long ways toward avoiding much trouble,” “Pogroms, persecutions and the mythical holocaust. They only get what they so very richly deserve.” Computer Bulletin Board Under Fire for Allowing Anti-Semitic Messages, Agence France Presse, Oct. 23, 1991, available in LEXIS, News Library, AFP File. Eventually, it was determined that this text never appeared in a publicly available electronic space on the Prodigy network but was transmitted in the private e-mail.
39. See, e.g., Prodigy Did Not Publish, supra note 33.
41. See Walker, supra note 38, at 36 (reprinting Prodigy public relations staffer’s chronology of reactions to the incident).
of a publisher editing content; in others it is delivering e-mail and acting as a carrier legally forbidden to monitor content; in others it is offering a public forum for the discussion of public issues; and in still others it is acting as a distributor that would not be required to monitor content. Thus, Prodigy and its counterparts represent a truly unique type of information utility. To impose existing legal metaphors on commercial information providers would be unwise without differentiating the ways in which these providers represent different modes of information transport, not all of which have real-world counterparts. In a digital data stream it is not easy to tell the difference between what, in former times, might have been a newspaper, or a cable television system, or a broadcaster, or a common carrier—each of which would have been entitled to its own legal regime and practicing bar. Nonetheless, it would be unwise to impose a generic legal regime clustering all of these legal metaphors into a single new legal metaphor purporting to serve as an overall umbrella for the Networld.

C. Imposing Local Community Rules on an Unyielding Cybercommunity

Unfortunately, as real-world cases arise with greater frequency, efforts to impose existing statutory laws and administrative regulations on these new cyberspaces and cybercommunities have become more common and more troublesome. The first case raises the issue of whose community rules should govern a cyberspace controversy, those of the existing geopolitical jurisdiction or those of the cybercommunity. In the area of pornography, the Amateur Action case has provoked consternation and concern among both network users and information providers. The Amateur Action BBS was a subscription bulletin board where users, consenting adults within an electronically mediated environment, could access pornographic materials. The images held to be obscene were uploaded in California and were downloaded in Memphis, Tennessee, deep within the Bible Belt where such pictures were considered objectionable and unacceptable under local community standards, the legal criterion on which obscenity determinations are based.

The attorney for the defendants, who operated the bulletin board, claimed that the trial was specifically initiated in Memphis rather than in California in order to take advantage of the more conservative climate prevailing in that

---

42. See Smith v. California, 361 U.S. 147 (1959) (finding that bookseller could not reasonably be expected to monitor content of all news vehicles it offered for sale and that to impose such requirement would restrict free circulation in information marketplace).

43. These information services would prefer not to use “utility” as a legal term of art because it suggests that they must offer their services to anyone. Most have long and comprehensive service contracts that specify what subscribers are to expect from them and what they expect of their subscribers. Thus, the relationship is construed as a license to use rather than an opportunity to purchase a commodity.

community. Indeed, it appears that the person downloading the images was recruited by the prosecution for the purpose of establishing the offense. The case raises the important issue of which local community's standards should apply—that of the uploading provider, that of the downloading user, or the community standards maintained by and within the virtual community on the electronic network. This case is currently on appeal to the Sixth Circuit Court of Appeals and may eventually reach the Supreme Court. If the Court does not consider this particular case, one similar to it will likely arise in the near future. Otherwise, Congress will have to determine whether the present rule should be maintained or whether one more appropriate for computer-mediated communications should apply.

Clearly, if there exists a genuine impact outside the electronic community with detrimental consequences within the local community, as when local children are used as models in online pornography, geographical jurisdictional rules should apply. Indeed, if an information provider permits local children to access the locally offending pictures by negligently failing to verify that the users are “consenting adults,” local jurisdictional rules might also apply. If the photographs are circulated only electronically within a group of consenting

45. Porn Trial, COM. APPEAL (Memphis), July 19, 1994, at 6A.
46. Id.
47. The Memphis case may not be as clear on the issue of “local community standards” versus “virtual community standards” as legal purists would desire. Some material was sent via the mails in response to a request from a local citizen, a postal inspector. Such cases often are decided upon the particularities of the special circumstances under which they arise, sometimes clouding the policy issues upon which the future of the legal system rests.
48. The Jake Baker case presents an example of online behavior with a significant impact within the local community. Jake Baker (née Abraham Jacob Alkhabaz), a twenty-year-old student at the University of Michigan, was recently arrested, arraigned in U.S. District Court, and held without bail for transmitting via the Internet what were alleged to be both obscene and physically threatening messages in interstate traffic in contravention of 18 U.S.C. § 875(c) (1988). See Peter Swanson, More Information on the Jake Baker Case, Feb. 16, 1995, available online at URL <http://krusty.ecs.umich.edu/people/pjswan/Baker/pete/pete2.16.html>. A lurid story describing rape, torture, and murder was posted by Baker in the alt.sex.stories Usenet newsgroup in early January. According to regulars on the Internet, such stories are not uncommon, but the differentiating factor in this case was that Baker used the real name of a classmate as the name for the subject in his story. The story was picked up by a sixteen-year-old female in Moscow, who told her father. Id. The father then related the story to an alumnus of the University of Michigan, who alerted school administrators. Id. The University Department of Public Safety obtained a written waiver of rights to search Baker’s residence and computer, and found e-mail messages between Baker and a correspondent in Canada that revealed plans to carry out some of the fantasies in the real world and indicated that the named female was readily available to be kidnapped and “‘knock[ed] . . . unconscious and put . . . into one of those portable lockers.’” U.S. Attorney’s Office, Eastern Dist. of Mich., Baker Press Release, Feb. 9, 1995, available online at URL <http://www.mit.edu:8001/activities/safe/safew/case/umich-baker-story/us-pres> (quoting Affidavit of Special Agent Greg Stejskal of the FBI). Prior to a scheduled hearing on Baker’s suspension from the University, he was arrested by federal agents. Id. According to these reports, however, there were only words exchanged within cyberspaces and no threatening acts in physical spaces, so this may very well be a challenging case for First Amendment scholars to analyze.

In another recent development, the FBI captured Kevin D. Mitnick, the original cyberpunk who earned his title by plaguing computer sites around the country for over a decade. See John Markoff, A Most-Wanted Cyberthief Is Caught in His Own Web, N.Y. TIMES, Feb. 16, 1995, at A1.
adults, however, libertarian philosophy would maintain that the rules of the "virtual community" should apply.

The second case also concerns the conflicting rights and authority of members of the cybercommunity and outsiders who exist in the real geographical community. This case also represents a geographical jurisdiction's imposition of administrative rules that may infringe the rights of members of the cybercommunity. Moreover, the case has important overtones for the real-world retribution that may accompany online behavior.

This case involved a male-only bulletin board, the Super Oak Leaf Online (SOLO), operated within the journalism department of the Santa Rosa Junior College in California. Roger Karraker, the faculty advisor of the college's student newspaper, the Oak Leaf, established the bulletin board in response to student requests. The bulletin board, which was available to only ten males, was intended to be operated under a pledge of confidentiality. One of the male participants broke the pledge and informed two women of derogatory remarks made about them on the board. Because no women were involved in bulletin board conversation, however, the women who were allegedly harassed were not participants on the board. In response to the ensuing conflict, other students, including members of the newspaper staff, came to Karraker's aid and purported to "defend the fundamental right to freedom of expression."

The legal tool employed to stop this allegedly offensive e-mail was Title IX of the Educational Amendments of 1972. The Office of Civil Rights of the Department of Education directed the college to "promulgate guidelines of appropriate conduct for users" and to "notify the users of their right to be free from harassment on the basis of race, color, national origin or disability and to be free from retaliation for protesting such harassment." Accordingly, the Office directed Santa Rosa to amend its Administrative Computing Procedures to read:

The computing facilities at Santa Rosa Junior College are provided for the use of Santa Rosa Junior College students, faculty and staff in support of the programs of the College. All students, faculty, and staff are responsible for seeing that these computing facilities are used in an effective, efficient, ethical, non-discriminatory and lawful manner.

51. Santa Rosa Junior College Oak Leaf, News Release (May 4, 1993) [hereinafter News Release], in Mike Godwin, Speech Code Proposed in Online Forum at Junior College, Sept. 28, 1994, posted to listserv <cyberia-l@birds.wm.edu> (on file with author).
All students have the right to be free from any conduct connected with the use of SRJC computing systems which discriminates against any person on the basis of race, color, national origin, sex, or disability.54

As a final footnote, Karraker was forced to take an administrative leave as a result of complaints about sex discrimination on the board.55

Is there any place in the Networld that is private? One does not need to be a sexist or a racist to wonder where one must go to bare one’s soul to one’s friends. Ironically, women at Santa Rosa initially requested an all-female bulletin board on which they could discuss subjects of interest without the intrusion of males; the male bulletin board was subsequently established so that males could converse online in similar privacy.56 There are many other uses for private spaces on educational networks, even networks supported by public funds. Examples include the discussion of potential appointees, promotions, and student grades. It seems clear that separate cyberspaces should be demarcated for public or private use and that the differences between them must be recognized. Some physical spaces, including designations owned by public entities, are recognized as closed to public discourse;57 there should be no constitutional barrier to providing private electronic spaces in which confidential exchanges may take place. On the other hand, private spaces are sometimes held to have assumed the role of the state by opening themselves to public access and thus providing a public function.58 In order to avoid confusion, a cyberspace needs to be clear whether it is a private forum or a public forum.59

These issues further raise the question whether service providers must monitor e-mail to ensure that they are not breaking the law by permitting users to deploy the system for nefarious purposes. This presents the horns of an almost insolvable dilemma. Should service providers be held responsible for what users do on the systems? According to two recent intellectual property cases, they should be.60 If so, a much more cautious management of

54. Id.
56. Big Sister Is Watching, supra note 50.
electronic speech of all kinds will ensue. To comply with federal legislation prohibiting discrimination, institutions may find it necessary to become snoops and censors, thereby exposing themselves to liability for acting contrary to the Electronic Communications Privacy Act, which prohibits such monitoring of e-mail. There is no consensus concerning the way to resolve such a conflict, but outcries against "the politically correct firing squad" are becoming louder:

The [Santa Rosa Junior College incident] casts a pall over computer communication, which is still in its infancy.

E-mail is fast replacing back fences as the place to exchange ideas and gossip. Its content should be treated just as tolerantly as any other speech, or we risk limiting a freedom we cherish.

Colleges cannot censor every student's E-mail. Nor should they be expected to try.

Our schools have no obligation to offer electronic forums for chat. But once offered, speech on these electronic grapevines should be as free as the words we speak.

Both the Amateur Action and Santa Rosa Junior College incidents illustrate the difficulty in applying real-world rules to cybercommunities without considering whether the imposition creates a greater burden than necessary, in the process impinging upon First Amendment rights of free speech and autonomy over one's conversational environment. A possible solution in the Amateur Action case would be to change the standards governing obscenity from the "local community" to the "virtual community." The Santa Rosa Junior College incident presents a more serious confrontation between two conflicting principles: freedom from gender discrimination and freedom for private spaces from the intrusion of state authorities. To follow the reasoning of Rowan v. United States Post Office Department, where is the castle that one can call home within the Networld?

D. Cyberjurisdiction and the Imposition of Electronic Retribution

I turn now to a set of cases in which "netizens" have addressed aberrant behavior in their own cybercommunities. Indeed, there is a rich experience governing the conditions for offering a new newsgroup, including a mechanism for voting upon the viability of such a group and determining whether it should

infringement because billboard used plaintiff's copyrighted photographs).

62. Lynn Ludlow, Don't Gag E-mail; Colleges Shouldn't Censor Their Students' Electronic Messages, S.F. EXAMINER, Sept. 29, 1994, at A-20.
63. 397 U.S. 728, 737 (1970) (upholding statute permitting U.S. Post Office to bar future mailings from sender) ("The ancient concept that 'a man's home is his castle' into which 'not even the king may enter' has lost none of its vitality . . .") (footnote omitted).
be moderated.64 “Netizens” have also occasionally enforced their mores against outsiders invading their cyberspaces in an “unacceptable” manner. Three recent cases, each generated by a very different incident, illustrate the potential for cyberjurisdictions to develop highly effective legal norms to enforce acceptable standards of conduct.

The first case involved advertisers seeking to impose their messages upon newsgroups in a manner considered abhorrent by the recipients. Commercial use was initially deemed unacceptable on the federally funded predecessor to the Internet. Over the years, however, some advertising on the network became tolerated.65 Today businesses all over the country are rushing to set up their very own “home page”66 on the World Wide Web. Wired magazine has set up an electronic version of its popular print version, inviting advertisers to be innovative in how they presented themselves to what was perceived to be a prickly audience of computer-literate users wary of traditional methods of advertising.67 Today, commercial use of the Internet is beginning to overshadow its academic and research uses. Nevertheless, the tradition of the “acceptable use policy” remains deeply rooted on the Internet.

Two lawyers, Laurence Canter and Marsha Siegel of Phoenix, who dared to challenge this tradition, created a spate of resentment when they “spammed”68 thousands of Usenet conferences on the Internet with advertisements for their legal services. Because many users subscribe to several of these conferences, what they experienced could aptly be described as “opening a mailbox and finding thousands of junk mail letters with postage

64. See, e.g., Ed Bailey, First Call for Votes (1st of 2), Oct. 12, 1993, posted to Usenet newsgroups news.announce.newsgroups, news.groups, misc.legal, misc.legal.computing, misc.int-property, comp.patents, alt.comp.acad-freedom.talk, and alt.privacy (calling for votes on proposal for new group to be entitled “misc.legal.moderated”).

65. Stephen Wolff, Director of Networking for the National Science Foundation, has explained that even though the “acceptable use policy” may not be conducive to profit-making activities on the NSFNET, it was interpreted as prohibiting only those services that did not enhance the purposes of academic research and productivity: “[T]he touchstone is utility to the research and education (R&E) community. It doesn’t matter if you charge for your service: you’re charging not for the NSF-funded facilities which are provided to both you and your clientele, but rather for the value you have added to those facilities.” Quoted in Josh Blackman, Netiquette Advertising, June 26, 1994, posted to listserv <cyberia-l@birds.wm.edu> (on file with author). In another posting, Blackman discusses appropriate places on the Internet for advertisements, such as “for sale” and “for rent” newsgroups and travel lists. Josh Blackman, Yes, but What About Mau?, July 2, 1994, posted to listserv <cyberia-l@birds.wm.edu> (on file with author). Blackman also warns against sending an advertisement for a condominium to a brain-surgeon mailing list, since brain surgeons might prefer to discuss attributes of brains rather than condos. Id. This seems to sort out the differentiation of purpose that triggered the massive reaction to the Canter and Siegel advertisements that were wildly posted to every kind of newsgroup available.


68. The term “spamming” is meant to evoke the image of someone throwing a slice of Spam at a fan and watching the pieces fly out in every direction. See Peter H. Lewis, Anarchy, a Threat on the Electronic Frontier?, N.Y. TIMES, May 11, 1994, at D1, D7.
due." Recipients were outraged. They sent irate e-mail messages posted to the lawyers' mailbox and "electronic letter bombs" designed to destroy the Canter and Siegel advertisements.70

Eventually Canter and Siegel's network provider ordered the pair off the network. Canter and Siegel have threatened to file suit based upon an alleged First Amendment right of access. They have not yet filed suit, however, because some law firms have refused to take their case71 and because they have found an alternative outlet for their energies. Although they were reputed to have garnered $100,000 in fees from new clients, Canter and Siegel have found a more lucrative return in the information marketplace by writing a book on how to advertise on the Internet. They have given up their legal practice for a consulting business that advises clients about this new and burgeoning area of commercial activity on the Internet.72

Despite these new ventures, Canter and Siegel have not been content to enjoy the benefits of what the netizens alleged to be their wrongdoing. On February 9, 1995, the duo struck again. They dispatched an electronic message advertising legal services to clear credit records to over 10,000 newsgroups. Subscribers logged on to their computers to find a message that read: "<ad>GUARANTEED CREDIT REPAIR BY LAW FIRM." Canter and Siegel also managed to put their message in the equivalent of the telephonic 911 call: a channel reserved for emergency messages considered important enough for all newsgroups to take notice. As if this interruption were not enough, the pair surreptitiously appended a signal that informed newsgroup systems managers that these messages had the approval of managers whose groups require such clearance before posting.73 In the real world, this could be considered forgery of permission or breaking and entering. Moreover, the duo also posted the advertisements to mailings lists of the Electronic Frontier Foundation, which are normally used to send foundation news to journalists and policymakers.74

In response to the first transgression, one user who called himself Cancelmoose designed computer software to automatically cancel such messages as Canter and Siegel posted.75 His software was not mobilized, but many netizens sent out SOS messages urging him to deploy the countermeasure.76 The response of the suppliers of Canter and Siegel's

---

70. One irate protester created a "Phantom Phone Beeper which called 40 times every night, filling the voice-mail system of the Canter & Siegel law office in Phoenix with electronic garbage." Peter H. Lewis, Sneering at a Virtual Lynch Mob, N.Y. TIMES, May 11, 1994, at D7.
71. Lawyers whom Canter and Siegel approached informed the author of this fact.
73. Martyn Williams, Spammers Strike Again on Internet, NEWSBYTES, Feb. 9, 1995 (on file with author).
74. Id.
75. Id.
76. Id.
Internet service was swift and final, as they pulled the plug on the massive mailing very shortly after it was detected. Such retribution as Canter and Siegel suffered, both the official acts of the service supplier and the vigilante acts of the angry subscribers, demonstrates that "spamming" of advertisements into Internet newsgroups has become a problem of mammoth proportions. What is most interesting, however, is the potential for self-governance and self-policing in cyberspaces that these events demonstrate.

Cybercommunities have also conducted online discussions of appropriate behavior, and imposed sanctions on violators, in the controversy over anonymous remailers. The fiercely held and opposing views regarding anonymity on the Internet expressed by this lengthy online debate have little or no counterpart in the real world. Two anonymous remailers, Johan Helsingius of Finland and Karl Kleinpaste of the United States, have sparred over the issue for many months. The argument centered around computer software that Kleinpaste wrote and shared with Helsingius. Helsingius began to use the software in a manner that Kleinpaste considered quite objectionable. The arguments between the two are enlightening and, judging from the number of postings that were entered into the electronic dialogue, aroused broad interest on the part of other users.

The need for pseudonymous messages originated in some of the more volatile discussion groups in which contributors did not wish to be identified, such as "alt.sex.bondage." The apparent need for anonymity motivated Kleinpaste to design an anonymous remailer system in six hours and to offer it to the "rec.nude" group, which declined his offer to serve their entire user membership. Undaunted, Kleinpaste deployed what he called a "fire extinguisher" to quiet abusive users against whom complaints were filed and used it three times before he was so "overwhelmed" by abusers that he decided to shut down his system. The server was not reestablished until April 1993, and then with a formidable list of forbidden uses.

David Clunie also devised an innovative anonymous posting system involving cryptography and offered it in October 1992. Complaints from a large U.S. site resulted in a warning to Clunie to shut down his system or lose

---

77. Martyn Williams, Spammer Attorneys Get Disconnected from Internet, *Newsbytes News Network*, Feb. 16, 1995, available in LEXIS, News Library, Curnws File. The contract that Canter and Siegel had with their Internet supplier, Performance Systems International, prohibited mass postings such as this, but their message was initiated from another source, Consumer Credit Advocates, with a return address for the Canter and Siegel e-mail box. Id.


79. See id.
80. Id. § 1.6.
81. Id. § 2.1.
82. Id.
83. Id.
84. Id. § 2.2.
his feed site. The allegation was that the anonymous server was dominating limited available bandwidth in the South Pacific and thus elevating expenses beyond justifiable costs, a charge that Clunie denied. Nonetheless, he discontinued operations in January 1993 but released his software into the public domain, where it could be recovered and used by others.

Meanwhile, in November 1992, Helsingius offered his own anonymous remailing site in Finland based upon code written by Kleinpaste. Although he intended to limit his service to Scandinavia, he found it tempting to respond to international requests for remailings spurred by "the lawsuit-intensive climate in the U.S.", where anonymous remailers were having a hard time surviving. With a commitment to providing anonymity to all Usenet groups, Helsingius has met with strong opposition from outraged managers as well as from vocal users who view anonymity as a threat to accountability and civility on the Internet. The strongest opposition came from Kleinpaste, who threatened to organize a vigilante group of irate news operators and to "arm the Usenet Death Penalty" to express objection to Helsingius' having introduced the anonymous remailing service without ascertaining whether the user community approved. This device has not yet been deployed, but the Helsingius server has crashed several times, at least once through "mailbombing" by anonymous protesters.

The argument concerning the desirability of anonymous remailing has not been settled and continues to occupy the time and attention of large numbers of net users. That there was a sizable demand for such service is undeniable: Helsingius was inundated with 13,000 registered users in his first three months of operation. Helsingius eventually shut down his service, bowing to network intimidation, although at the time of shutdown he was forwarding 3500 messages per day to 576 newsgroups. He also expressed great concern that "the strongest opposition to the service . . . came from network administrators." Ironically, much of the opposition was expressed by anonymous objectors in messages similar to the following:

I am drowning in a backlog of work, so I can't go into all the details here, nor am I particularly interested in entering into a long debate—the bandwidth is too low and my time is too constrained. I

---

85. See id.
86. See id.
87. Id.
88. Id. § 2.3.
89. Id. (quoting Helsingius).
90. Id. (quoting Kleinpaste).
91. Id.
92. Id.
93. Id.
94. Id.
do not believe we have the appropriate technology to make an anonymous service work on the net.

I am a firm believer in privacy, but that is not the same thing as anonymity. Anonymity can be used to violate another's privacy. For instance, in recent years, I have had harassing anonymous notes and phone calls threatening XXX because of things I have said on the net. I have seen neighbors and friends come under great suspicion and hardship because of anonymous notes claiming they used drugs or abused children. I have seen too many historical accounts of witch-hunts, secret tribunals, and pogroms—all based on anonymous accusations. I am in favor of defeating the reasons people need anonymity, not giving the wrong-doers another mechanism to use to harass others.

... You will not find the recipients of anonymous mail being the supporters of such a proposal. If the only people who would support the idea are those who might use it, is it proper?

The debate continues concerning what level of anonymity should be permitted in cyberspace, when, and under what circumstances. One might propose that the international community prohibit anonymous remailers. Some more discerning analysts of the cyberscene have suggested that servers who choose to provide an anonymous service should be held responsible for abusive messages posted on the system, since the real abusers would not be identifiable except through the entrepreneur providing this service. Therefore, one might distinguish between potentially hazardous message sources and other more innocuous uses of anonymity, thereby enabling the law to insulate from liability the majority of information providers while imposing liability on those originating the abusive messages.

As the tortured history of anonymous remailers indicates, net users have their own methodology for determining what is considered appropriate behavior, and they tend to favor tolerance rather than strict accountability. Furthermore, they often take enforcement of their standards into their own hands and seem quite capable of doing so without the help or intrusion of lawyers or judges from the real world.

Finally, the third case demonstrates that cybercommunities at times resort to the age-old remedy of excommunication for those who are simply unable to conform their conduct to the minimum level of acceptability. Historically,

95. Id. (quoting posting of John Noring, systems operator who provided excerpts from e-mail of anonymous user).
96. Conversation with David Johnson, Chairman, LEXIS Counsel Connect (Feb. 1995).
97. Geopolitical jurisdictions, however, are not standing aside in these matters. In February 1995, acting on a request from INTERPOL, the Finnish police obtained a search warrant and retrieved the name of a user of the Helsingius' server who allegedly had posted copyrighted material pirated from the Church of Scientology. See Anon.penet.fi Compromised, Feb. 18, 1995 (on file with author). While offering users an opportunity to remove their names from his files, the anonymous administrator sought support from his users to fight Finnish authorities. Id.
“shunning” or excommunication has been a very effective strategy for curtailing the speech or undesirable activities of citizens who do not conform to the cultural norms of their community. Whether virtual communities are justified in excluding undesirables on the basis of their speech is a legitimate question to be included in the assessment of the collision between the deployment of new media and the preservation of First Amendment values. Furthermore, if private cyberspaces and privately owned information service providers may exclude whomever they like, are public institutions obligated to provide public forums for the discussion of issues that affect the body politic?

A case in point is the virtual rape on the LambdaMOO (MOO). Mr. Bungle (a pseudonym) committed sexually explicit verbal rape on a female in a public space and was appropriately chastised for his behavior. In actuality, the Mr. Bungle persona took over the characters created by other participants in the MOO and attributed to them sadistic fantasies that highly offended them and others. After much discussion and consternation, especially with respect to what constituted a proper trial and due process, the Wizards (the skilled computer literati) in the MOO decided that there was a consensus that Mr. Bungle should be “toaded” (in fairy-tale terms, turned into a frog). As many as fifty or so of the MOOers verbally seconded the motion to “toad” Mr. Bungle, with only a dozen or so hard-liners objecting. As a result of his punishment, Mr. Bungle was banished from the MOO into oblivion.

What concerned the members of the LambdaMOO after the incident was resolved was how to handle such aberrant behavior in the future. The first question they faced was what constituted a community of citizens in the

98. The LambdaMOO was a multiuser dimension established for a group of professionals admitted on the basis of their academic qualifications and interests in multimedia. Amy Bruckman, Presentation at MIT Communications Forum on Democracy in Cyberspace, in Cambridge, Mass. (May 5, 1994). The aberrant behavior at issue in this controversy offended the participants not only because of what they considered to be obscene behavior but also because it fell beyond the scope of the intended use of the medium.

99. See Julian Dibbell, A Rape in Cyberspace, VILLAGE VOICE, Dec. 21, 1993, at 36 (providing detailed description and analysis of this “MUD rape” and reactions to it). What concerned the participants in the MOO was that Mr. Bungle was able to take control over the persona of the individual and describe in salacious detail sexual behavior that was highly offensive to those who were subjected to the textual rendition of his sexual fantasies. See id. at 37–38.

100. A female participant from Haverford, Pennsylvania, whose account identified her character as “Starsinger,” was displayed on the computer screens of all MOOers in words that read, “As if against her will, Starsinger jabs a steak knife up her ass, causing immense joy. You hear Mr. Bungle laughing evilly in the distance.” Id. at 38. Another character identified as “legba” suffered a similar form of sexual degradation. See id.

101. “Toading” normally refers to changing the attributes of the character selected by the participant in the MOO into the attributes of an amphibian. Id. at 39. In this case, however, “the annihilation of the character” was more permanent, erasing all of the attributes of the character and deleting his account on the MOO. Id.

102. Id.

103. Id. at 41. In fact, he went out and acquired another account on the Internet and reentered the LambdaMOO some months later, with a new pseudonym, attributes of a modified persona, and a more acceptable behavior pattern. Nonetheless, his behavior was similar enough for the other members to suspect that Mr. Bungle was amongst them once again. Id. at 41–42.
Moreover, they needed to determine how to empower themselves to set standards of behavior within the community they defined. The experience of witnessing and rejecting the behavior of Mr. Bungle precipitated a crisis in governance that prompted the group to consider what kind of social organization they wished to live under in the future. Some users, "[p]arliamentarian legalist types," argued that Mr. Bungle should not have been "toaded" because he had not broken any preexisting rules but also urged that a regimented system be inaugurated. Others argued that behavioral standards were a matter of individual choice, and that those who objected to Mr. Bungle's behavior should merely close their eyes or "hit the @gag command," blocking all of the messages from Mr. Bungle from their screens. The latter alternative, however, merely eliminates the message from the view of the offended but leaves the real individuals using the "Starsinger" and "legba" identities unprotected from the misrepresentation that they were the sources of the reprehensible language.

Amy Bruckman, a graduate student at MIT who is writing a Ph.D. dissertation on electronic communication, has discussed the agonies of the LambdaMOO participants concerning their deliberations about the fate of Mr. Bungle. She said that she did not have as much time as many of the other participants to spend on the MOO discussing what to do about Mr. Bungle, but that she was not willing to waive her right to participate in the decisions to those who did. This reflection on the process, in which the participants on the MOO engaged themselves for many hours, raises some unanswered questions about the viability of computer-mediated communication as a medium for a democratic process. What constitutes a fair and equitable process for determining who should be permitted to participate in electronic discussions? How many participants can participate effectively in democratic decisions? Is there a rational way to appoint representatives? Should we assume that consensus will be reached through mediation and that those who care enough to participate will do so while those who prefer to lurk will make known their preferences only when they become riled up enough to express them?

In the United States, unlike some other countries, citizens are not required to vote. Some political scientists believe that democracies work best when only those who care go to the polls. Thus, a democratic system may be sustained

104. Id. at 39.
105. Id.
106. Id.
107. Id.
108. See Bruckman, supra note 98; see also Dibbell, supra note 99. "[T]he question of what to do about Mr. Bungle began to shape itself into a sort of referendum on the political future of the MOO."
109. Id. at 39.
110. Bruckman, supra note 98.
by those with sufficient motivation to care about its future. There simply is not yet sufficient experience in the Networld to come to any conclusions about the viability of electronic democracy. Nonetheless, the Internet is a hotbed of experimentation on how to achieve this end, peopled with dedicated computer-competent users who believe that they have discovered a superior way to achieve consensual governance of cybercommunities without the aid of real communities. Indeed, given the proprietary propensities of those who use computer-mediated communication regularly, they would be the most unlikely candidates to relinquish control over their cyberspaces to an outside geopolitical jurisdiction.

E. A Case that Has No Cybersolutions

There are many troublesome cases arising in cyberspaces that may require innovative solutions. These may challenge the budding cyberlawyers to come up with some new remedies, and netizens will likely mold their own responses. One such case involved the use of aliases and pseudonyms. This practice is quite common on many bulletin boards, and despite the often abusive behavior that these names facilitate, no real solution to this problem has been found.

The “Strange Case of the Electronic Lover” involved an alleged female who suggested the establishment of an all-female bulletin board on CompuServe in which women could talk frankly with one another. The female who suggested the special interest group was allegedly confined to a wheelchair. She identified herself as Joan Sue Green and claimed she was a New York neuropsychologist who had been injured in an automobile accident caused by a drunk driver. The women on the electronic discussion confided their innermost sentiments to her. Indeed, Joan discussed her sexual inclinations quite openly and encouraged others to do the same. “Joan” also quite openly suggested that they meet a “friend” of hers, a psychiatrist named Alex. As it turned out, Alex, a prominent New York psychiatrist, was in reality the “Joan” of the discussion group. When the other participants realized how they had been fooled by the psychiatrist, they felt violated and betrayed. Nonetheless, they had to admit that “Joan” had been able to help many of them sort out their problems.

This case is only one of many that have heightened concern about the threat of anonymous messages, an aspect of computer-mediated communication.

---

112. Id. at 101.
113. Id. at 94.
114. Id.
115. Id. at 101, 103.
116. Id. at 103, 117.
117. Id. at 99.
118. Id. at 104-05.
that probably can never be completely eliminated. Discouraging anonymity would have the therapeutic effect of labeling anonymous messages as undesirable and, perhaps, reprehensible. There are, however, appropriate uses of anonymity that should not be discouraged. The challenge is to distinguish between the categories and draw the protective prohibition as narrowly as possible. Certainly the use of electronic chat channels by pedophiles to solicit the companionship of young computer users is one that most observers would abhor. This problem might be mitigated, however, by posting warnings to children to avoid real meetings with their virtual friends until they have some verification of their real identities and intentions, as well as vigorous enforcement of real laws. Such solutions would seem to provide a better way of dealing with this problem than forbidding all uses of aliases and pseudonyms in electronic playgrounds.

The case of “Joan” has not precipitated the irate response from the deceived parties on the CompuServe network that one might have expected, considering the rather prompt response taken by active participants on some of the Internet newsgroups. Perhaps this is because the forum was inhabited primarily by females, purported, at least, to be more gentle in their objections than their male counterparts. Perhaps it is because they all felt embarrassed, or somehow to blame, for not recognizing the imposter in their midst. Perhaps they saw no way to impose effective sanctions. Or they may have merely succumbed to the notion that pseudonymity is a fact of life in the Networld and that users should therefore be careful to scrutinize the messages of unidentifiable correspondents.

It is unlikely that the impostor would have asserted a First Amendment right to post the messages under an assumed name in this cybercommunity. But the incident demonstrates the need to determine at what points on the continuum of anonymity censure will fall. It seems easier to evaluate appropriate responses to anonymity at the extremes. For example, some anonymous users may use their anonymity to be rude and impolite, but such activity may not qualify for removal from the cybercommunity. Similarly, the destructive and potentially dangerous uses of anonymity also are relatively easily identified and sanctioned. The questions become more difficult as anonymous usages approach the center of the continuum, where anonymity becomes a problem, but is not necessarily totally unacceptable. These questions will challenge cybercommunities to devise rules and standards to govern the uses of anonymity in their electronic neighborhoods.

III. SELF-GOVERNANCE: THE POSSIBILITY OF CYBERJURISDICTION

Users of cyberspaces are exercising some autonomy over their cybercommunities and beginning to apply their own customs and practices to
abusive or troublesome behavior. Moreover, several cyberconversations have specifically addressed questions of cyberjurisdiction and the development of cyberlaws. During the Summer of 1993, Professor Trotter Hardy, of the Marshall-Wythe School of Law at the College of William and Mary, began one such conversation by asking whether it would be possible to develop and enforce a constitution for cyberspace. Professor Hardy received some severely critical postings protesting the invasion of real-world legal metaphors into these new cyberspace communities. Although some deplored the thought of regulation rearing its ugly head in the Networld, especially since the real world was experiencing a progressive trend toward deregulation, Hardy viewed the proposal as a potential means for insulating the Networld from the real world. He explained that a constitution could actually protect the cyberspaces rather than make them vulnerable to excessive external regulation; a constitution might proclaim that "No one can regulate anything anybody does on the nets."" In September 1993, Professor Hardy assembled a more selective listserv group of approximately twenty lawyers to spend several weeks online discussing the possibility of exercising independent jurisdiction over cyberspaces that might be immune to territorial law. These pioneers agreed to discuss some issues of real-life import in the cyberspaces. Recognizing that potential intrusion by territorial jurisdictions is fast approaching, the

119. See, e.g., Rheingold, supra note 8, at 64 (describing informal community self-regulation as "Netiquette").

120. Professor Hardy summarized many of the responses to his query in a posting entitled Constitutions, Magna Cartas, More (on file with author) and the conference came to be known as "Cyberia."

121. One such message read: ""Re A Constitution for Cyberspace. Eeeeeeeekkkkkkkkkk. You have ruined an otherwise perfect, harmonious and anarchist day on the nets. Let's not do it and tell all the author[ar]ian types that we did, ok?"" See id. (quoting message as not atypical reaction to his query regarding cyberspace constitution).

122. Id.

123. A listserv is an e-mail list of people assigned access to a particular discussion group. Some are open, and anyone may subscribe. Others are closed, and would-be users must obtain permission to be included. As this one was by invitation, it was not open or available to outsiders. Thus, the participants were assumed to be computer literate and at least sometime users of the Internet or other commercial online services. The gateways enabled participants to post from a number of sources, including Prodigy, CompuServe, and America Online as well as direct accounts on the Internet. The conference was entitled the "NEWJURIS" conference and messages were dispatched to <newjuris-l@birds.wm.edu>. Participants included the following: Don Berman, Jerry Berman, Anne Branscomb, John Dale, Mike Godwin, David Johnson, Ethan Katsh, David Maher, Bill Marmon, Peter Martin, Charles Merrill, Abdul Paliwala, Henry Perritt, Ed Richards, Lance Rose, Marc Rotenberg, Pam Samuelson, Shari Steele, Cleve Thornton, Robin Widdison, and Ian Wilson. Messages quoted from this electronic stream are not attributed to particular parties because the participants agreed that this conference would be confidential so that members could speak freely without concern about being quoted either accurately or inaccurately in other environments.

124. See A NEW JURISDICTION FOR CYBERSPACE? A TRANSCRIPT OF NEWJURIS, AN ELECTRONIC CONFERENCE HELD SEPTEMBER–OCTOBER 1993 (Trotter Hardy ed., 1994). Professor Hardy began the conference with this introduction: ""The question at hand is whether cyberspace should form its own jurisdiction. But before we try to come to an overall conclusion, we would do well to start thinking in terms of pro's and con's. What would be good about treating cyberspace as a jurisdiction of its own? What would be bad?"" Id. at 2.
participants turned to serious consideration of the issues that might present different problems in cyberspaces than they do in the real world, the questions that are likely to find similar resolution in both worlds, and possible means of facilitating dispute resolution within cybercommunities without resorting to real-world courts for litigation. One participant noted at the outset that the netizens had already begun to develop self-governing jurisdictions, and he cautioned that the laws to govern interactions in the Networld should be established by those who understand and participate in the electronic world.¹²⁵

Participants in the NEWJURIS conference discussed various procedural elements of governance, such as whether providers of cyberspaces should post their rules of behavior.¹²⁶ There was also debate and dialogue regarding who ultimately had the power to make, amend, and adjudicate the rules, and these discussions in turn implicated questions of the potential for democratic discourse between providers and users of the cyberspaces.¹²⁷

Others questioned whether rules of geopolitical spaces concerning equity of access should apply to cybercommunities and whether cybercommunities could waive external rules against sex, gender, or racial discrimination.¹²⁸ Discussion also focused on the rights of cybercommunities to expel members who abused the privilege of participation.¹²⁹ Clearly, there was no consensus about what the rules should be in cyberspaces. There was agreement, however, that these budding cybercommunities should be given a chance to develop and test their own rules before the external authorities exert too heavy a hand to bring them into conformity with real-world rules.¹³⁰

There was also consensus that existing legal constructions, such as the law of associations,¹³¹ or historical experiences such as the law of merchant of the Middle Ages,¹³² or the experiences with customary international law, could apply comfortably to cybercommunities seeking to establish a set of cyberlaws that would not infringe upon the rights of citizens living outside these communities.¹³³

¹²⁵ Id. at 2 (posting of Sept. 20, 1993).
¹²⁶ See id. at 53 (Trotter Hardy’s summary of issues discussed during the conference).
¹²⁷ Id.
¹²⁸ Id.
¹²⁹ Id.
¹³⁰ Id. at 48–49.
¹³¹ Id. at 51.
¹³² Id. at 23 (posting of author, Sept. 24, 1993).
¹³³ In a conference on LEXIS Counsel Connect called The Law of the Electronic Road, this author’s parting posting was:

I have lurked here among you budding cyberlawyers without time to offer much comment. Although I find many interesting views, astute comments, and sage observations about what might become the law of cyberspace, I find very little comprehension or discussion of what is actually happening in cyberspaces. There is much customary law developing among the cyberresidents in their various communities without much help from the legal profession which has not shown much evidence of interest or participation until recent entry of commercial (read "potential clients") in these new electronic realms. I suspect that we will see and are seeing a
Not everyone agreed, of course, and it is wise to remember that not all
cybercitizens are conformists. Indeed, the most vocal are often not. As one of
the participants wisely reminded his more optimistic colleagues:

There are always the hard cases, the ones who won’t play ball unless
they see a baseball bat about to whack them in the head. While the
nice people are agreeing, those inclined to disagree will have free run
of the net. I doubt that unforced agreement is sufficient; rather, to
create workable net regimes, someone or some group will need to
wield the power necessary to herd malcontents into line.\textsuperscript{134}

Professor Hardy, in summary, recognized that “creating a law of
cyberspace is fraught with difficulty,”\textsuperscript{135} but this did not deter him from
going forward and sorting out many of the differences between those areas in
which geopolitical jurisdiction seems to apply comfortably in
cybercommunities (such as defamation)\textsuperscript{136} from those in which it does not
(such as imposing a publisher’s responsibility for the content of many user-
originated messages).\textsuperscript{137} In general, however, Professor Hardy endorsed a
newly emerging “Law in Cyberspace” coexisting with statutory law governing
dependence on the geopolitical.\textsuperscript{138}

Other more open conferences have not reached such benign conclusions;
some have recognized the emerging law while not calling it that. For example,
while recognizing that some law of the wild reigns, with each individual sysop
acting as the Lord Chancellor and High Executioner, some observers have also
noted that there are real, operative rules being promulgated all the time in
cyberspace communities:

“There are already many such constitutions. I have only begun to
cruise the MUDs (and MOOs, MUSEs, MUCKs, etc.). However, each

\textsuperscript{134} Lance Rose, \textit{Consensus or Force}, May 18, 1994, available online at LEXIS Counsel Connect, Discuss Menu, National and International Topical Forum, Computers & Technology Law, Networks and Online Services.

\textsuperscript{135} Anne Wells Branscomb, \textit{Addenda to Discipline}, Dec. 8, 1994, posted to LEXIS Counsel Connect, Discuss Menu, The Law of the Electronic Road Seminar (on file with author).


\textsuperscript{137} Id. at 1004–06.

\textsuperscript{138} Id. at 1021.
seems to have its own credos and rules. These laws are frequently HEAVILY enforced.

... Finally, even mailing lists and news groups have some set of laws (NO FLAMES, STICK TO THE TOPIC, etc.). I'm not sure how one would unify all such rules under a universal or meta set of rules."

What is different about communication in cybercommunities from communication in geopolitical communities is the opportunity for an individual to become a producer as well as a receiver of information. Mass media (such as newspapers and broadcasters) permit single-source communication to multiple receivers, while common carriers (such as postal, telegraphic, telephonic, and facsimile messages) permit single-source communication to single or multiple receivers. In contrast, computer-mediated communication is a many-to-many system of distribution. This difference was expressed quite eloquently by Mike Godwin, Legal Counsel for the Electronic Frontier Foundation:

What all these systems, from the smallest single-line BBS to the Internet, have in common today is their reliance on text. . . . Computer users have grown more adept at effectively writing to each other. The world of the networks is a true democracy: your influence is measured not by wealth or position, but by how well you write and reason.

This reliance on the printed word is, of course, something that the computer-based services share with the traditional print media. But they differ from print media—and broadcast media—in two very important ways. First, the means of communication are cheap enough for almost everyone to gain access . . . [Second.] Computer information services . . . are "many-to-many" systems . . . The "filtering" function performed by newspaper editors is left to the readers, who are also contributors. The very distinction between reader and "reporter" is blurred.

This may sound like anarchy, but in practice it's more like a town-hall meeting, albeit one in which everyone has a chance to speak, no one is shouted down, and people have time to develop and explain their ideas.

Godwin's model is treasured by many of the "netizens" who share the faith that the Networld in which they are creating their cybercommunities offers a new opportunity to realize the democratic ideals with which the Founding Fathers established and created new communities on the North

139. Hardy, Constitutions, Magna Cartas, more, supra note 120 (quoting response to his initial inquiry).
140. See NATIONAL RESEARCH COUNCIL ET AL., RIGHTS AND RESPONSIBILITIES OF PARTICIPANTS IN NETWORKED COMMUNITIES 40 (Dorothy E. Denning & Herbert S. Lin eds., 1994).
American continent. This is not an unruly model or electronic anarchy but one of civil and thoughtful discourse leading to consensual governance. The road is rocky, however, and clashes will continue to plague the pioneers and settlers as the abuses of cyberspaces come to be viewed as growth opportunities for litigants and lawyers. As Professor Hardy has commented: "The golden age of cyberspace is ending, but the golden age for lawyers is just dawning." In contrast to Hardy’s prediction, Benjamin Wittes, a lawyer who moderates an online forum for lawyers, observed that the role of the lawyers might have been usurped by the netizens of cyberspaces:

Suppose you wanted to witness the birth and development of a legal system.
You would need a large, complex social system that lies outside of all other legal authorities. Moreover, you would need that system somehow to accelerate the seemingly millennial progress of legal development, so you could witness more than a mere moment of the process.
This hypothetical system might seem like a social scientist’s fantasy, but it actually exists. It’s called the Internet.

IV. THREATS TO AN ONLINE AGORA: RETHINKING SOME PRINCIPLES OF FIRST AMENDMENT PRACTICE

Many users and proponents of online computer communication tout its capability as the best means by which to achieve the goals of a democratic society. With the opportunity for anyone with access to a computer connected to a modern and a telecommunications system to reach anybody or everybody else so equipped at any time, anywhere, the many-to-many form of communication outperforms all other existing media in its potential utility for electronic democracy. Far from the mass-media mode of newspapers and broadcasting, with their limited interactive responses through letters to the editor and talk television, computer-mediated communication offers open access to uploading messages (speech) and open access to downloading information (also speech). True, there may be a cost associated with this capability, although it is essentially no different from the price of newsprint or television sets. Nonetheless, the political pot of gold at the end of the rainbow seems reachable within the foreseeable future, given a commitment to universal access at least through publicly available terminals and computer-assisted

142. Quoted in Tony Mauro, Riding Herd On-Line: Legal Notions Transformed by Digital Age, USA TODAY, Nov. 15, 1994, at 1A; see also Mark Eckenwiler, Criminal Law and the Internet, LEGAL TIMES, Jan. 23, 1995, at S32 ("If 1994 was the Year of the Internet, 1995 promises to be the Year of Legal Questions About the Internet.").
143. Benjamin Wittes, Law in Cyberspace; Witnessing the Birth of a Legal System on the Net, LEGAL TIMES, Jan. 23, 1995, at S27.
education. This makes the Networld an attractive conduit for democratic discourse.

Indeed, the experiences of Internet, Prodigy, CompuServe, America Online, and the tens of thousands of sysops demonstrate a remarkably diverse marketplace of ideas bubbling up all over the globe. The Networld has an abundance of opportunities for full and uninhibited speech. The difficulty has become one of offended parties seeking to inhibit the speech of the offending posters of messages. As the offended turn to their lawyers to redress their grievances, this uninhibited cauldron of opinion becomes threatened. Should strict liability for all electronic transmission become the accepted norm, service providers might scramble to hide behind contracts, waivers, monitoring of all content, and censorship of messages before posting. Such developments would effectively exclude the majority of the smaller sysops who may operate a board mainly for their own personal interests or as an appendage to a hobby club or a small business. Liability insurance would be prohibitively expensive, the burden of monitoring all messages before posting them too demanding, and the possibility of facing protracted litigation too onerous. To foreclose in this manner a most interesting experiment in democratic discourse would be disheartening and disillusioning. Is it not possible to find some other way of moderating abuses of computer-mediated communications systems? Following are some suggestions for doing so.

A. A Right of Reply for Defamation

A right of reply has been urged and rejected in the print media, and tried, approved and then abandoned (at least partially) in the broadcasting media. Nonetheless, there is a need to find some alternative to strict liability for providers of information services without imposing an obligation to monitor all messages in order to avoid incurring provider liability. Thus, the return to a right of reply, affirmed as constitutionally acceptable in Red Lion Broadcasting Co. v. FCC, seems eminently reasonable. The general counsels of both Prodigy and America Online have explained that they see no other viable alternative than offering defamed parties an opportunity to

come online and defend themselves in the channel where the alleged defamation has taken place.\textsuperscript{149}

To do otherwise would have a chilling effect on the medium, where the very large amount of traffic makes it almost impossible for an information provider to monitor. If the electronic messaging services are required to accept responsibility for all of their content—as are "publishers" in the print and broadcasting world—then a budding electronic democracy of free speech operating in an electronic "public forum" may be lost. At the very least, it should become possible for electronic information providers to declare some cyberspaces to be "public forums" where messages may be circulated freely. Otherwise the public forum, as modeled on the ancient agora, may be lost as an uninhibited "marketplace of ideas."\textsuperscript{150}

B. Displacement of the Local Community's Standards by the Virtual Community's Standards

The Amateur Action case has highlighted the difficulty of applying geographically local community standards to a computer bulletin board. Such pornographic images as were involved in this case, coming as they do from diverse locations all over the globe, create no harm to any local population unless and until the local population becomes a part of the computer-mediated traffic. Even then, unless one can argue that exposure of adults to the images creates a clear and present danger to the local community, such as inciting to rape or assault, the user creates no local disturbance assuming that the images merely are viewed and not downloaded, or once downloaded, not distributed. Changing the standard from local to virtual community would seem reasonable as long as the users of the networked images are a contained user group of consenting adults who are screened for admission to the circle of participants.

The Santa Rosa Junior College bulletin board case offers another opportunity to review whether the standards of the geopolitical jurisdiction or the standards of the cybercommunity should govern behavior in the cybercommunity. This case raises substantial doubt about the autonomy of cybercommunities to patrol their own boundaries even when the behavior within the cybercommunity does not have a deleterious impact upon the real world. Whether this case fits into this category is debatable, but at a minimum

\textsuperscript{149} Conversation with George Perry, General Counsel, Prodigy, at the Workshop on Rights and Responsibilities of Participants in Networked Communities, in Washington, D.C. (Nov. 5-6, 1992); Conversation with Ellen Kirsh, General Counsel, America Online, Inc., at National Conference of Lawyers and Scientists, Conference on Legal, Ethical, and Technological Aspects of Computer Use and Abuse, in Queenstown, Md. (Oct. 7-9, 1994).

\textsuperscript{150} For a fuller discussion of the problems of the "public forum" concept, see Goldstone, \textit{supra} note 59.
it affords another vehicle by which to explore issues of community definition and self-governance.

C. Defining Information Privacy as Sanctity, Autonomy, and Confidentiality

There is a great deal of confusion about what privacy means, what information can be protected from disclosure, and whether unwanted messages may be prevented from intruding into private spaces. It is clear, however, that there is growing public demand for assurances that personal autonomy over private information will be respected and that personal transmissions will be kept confidential. It is also apparent that public expectations of some modicum of sanctity of personal space should be guaranteed. What this space constitutes in a legal sense and how much control over it the individual may exert has not yet been determined.

First Amendment scholars could engage in a useful public service if they would concentrate on defining these emerging legal boundaries rather than criticizing and rejecting the meager legal structures that currently exist. Practical solutions would be more speedily devised if it were possible to focus the arguments about what constitutes a sanctified personal space around which an individual may draw an electronic boundary. Privacy scholars should also be more precise in distinguishing two different types of information-autonomy problems. The first paradigm concerns those releases of information that are deserving of some level of legally enforceable confidentiality. The second category involves group assertions of autonomy to block outside intrusions into cyberspaces that they wish to limit to certain types of information transfers. The latter situations bear some resemblance to the zoning of real property. Thus, "infozoning" may become a growth area of the law. A difficult challenge, however, is to treat different cyberproblems differently, without seeking to find simple, universal solutions to all of the new questions.

D. First Amendment Rights of Association and Access Online

The SOLO bulletin board incident at Santa Rosa Junior College has precipitated a reappraisal of the responsibilities of network managers to monitor and patrol the traffic within the computer-mediated setting. If the provider is to be held accountable for how an electronic space is being used, then there can be no such thing as a private electronic space, except within private networks offered and funded by private entities (such as individual bulletin board providers). Educational institutions do not monitor the speech of their students within their dormitory rooms, dining halls, playing fields, or locker rooms. Why should it be necessary to monitor electronic bulletin boards?
Surely there is a rationale for protecting freedom of association and speech in the sense of preventing federally funded entities from interfering with what is spoken in an electronic space. No one would condone derogatory speech by males about females or vice versa, but the speech involved in the SOLO case seems to fall in the category of good manners and conduct expected of a desirable member of the collegiate community rather than an infringement of federally protected civil rights. Gender-specific, national, racial, and religious groups have legitimate reasons for desiring some autonomy over electronic space in which to discuss group-specific issues.

E. Should Commercial Messages Be Permitted in E-mail Traffic?

The experience with the overabundance of commercial messages from the Canter and Siegel firm in Phoenix has highlighted the difficulties of assuming that the practices acceptable in other media will transfer comfortably to electronic media. With “junk mail,” the current expectation is that it can be tossed into the wastepaper basket unopened without cost to the recipient. Only the poster of the paper message pays for delivery. In the context of electronic mail, however, the recipient pays for the service in which the message is posted and often not only is charged for the space but also has a limited space in which to file incoming messages. Furthermore, it takes time to download messages from the e-mail depository. Thus, if large numbers of people followed the example of Canter and Siegel in “spamming” every newsgroup in sight, the results would be intolerable.

Prohibiting the posting of e-mail advertisements into newsgroups with assigned topics under discussion would seem reasonable, because such inundation is disruptive, intrusive, and surely an invasion of the sanctity that the Supreme Court purportedly protected in *Rowan v. United States Post Office Department*. In actuality, however, the opportunity to place advertising copy into the electronic space, much as advertisements are placed in newspapers, exists on the Internet and may be facilitated by commercial information service providers. Although the eye may scan advertisements in the newspaper columns, there is neither compulsion to read nor any cost associated with receiving such reading material, other than the cost of the newspaper itself. Home pages on the World Wide Web or similar servers would provide adequate access to electronic viewers who may at their option choose to seek out the advertisements and services of providers with whom

---

151. This assumption is not entirely accurate since many communities charge for the pickup of wastepaper and garbage, and some waste services charge by the weight or number of bags. The author lives in such a community. In addition, environmentalists protest the number of trees cut down in a useless deployment of paper that is unread and wasted. See Jill Smolowe, *Read This!!!!!!!*, TIME, Nov. 26, 1990, at 62, 64.
they wish to deal. Consequently, prohibiting the delivery of commercial messages to e-mail destinations would seem consistent with the First Amendment's goal of encouraging a diversity of information sources without intruding upon the sanctity of personal e-mail or autonomous-group cyberspaces.

F. Should Anonymous Messages Be Discouraged?

Questions about the propriety of anonymity in the cyberspaces must be evaluated along a continuum. Anonymity should not be outlawed as a general principle; there are varying levels of anonymity, or at least pseudonymity, that are rational and justifiable. Permitting anonymity for the purpose of removing any vestige of accountability for abusive behavior, however, is not likely to be tolerated in the Networld. Whether or not anonymity is to be permitted or even encouraged depends upon the particular circumstances under which it is deployed, but it must be understood that many netizens are unlikely to waive their perceived right to personal autonomy, which some define as a right to genuine anonymity. The introduction of a bill into the 104th Congress by Senator Jim Exon (D-Neb.) to prohibit anonymous messages "with the intent to annoy, abuse, threaten, or harass any person . . . who receives the communication" has prompted a spate of controversial discussions on the Internet.

The anonymity question is further muddied by a great deal of confusion about what constitutes privacy in electronic communication. The agitation regarding the use of high levels of cryptography to protect the "privacy" of electronic messages should not be confused with the question of true anonymity of message sources. The "pretty good privacy" software favored by Internet users, as well as the hostility to anonymity-stripping devices such as the Clipper Chip and Wire Tap, are not directed at ensuring anonymity. Rather, they reflect efforts to protect the confidentiality of message content from the intrusive eyes of outsiders and to protect the transmission of a message between consenting parties.

Presumably, commercial information vendors and service providers would be free to set their own rules governing the anonymous posting of messages, defining the appropriate uses of aliases and pseudonyms, and demarcating the electronic channels in which such uses would be acceptable. Furthermore, commercial services, including commercial anonymous remailers, must know who their customers are in order to bill them or their legal representatives or agents. Thus, the local or national laws of the host nation or state could provide mechanisms for subpoenaing the identities of customers who abuse the privileges of pseudonymity and contravene local law. A nation-state would have to cooperate in applying its own laws, but some nations might refuse to

do so, offering instead a national data haven to attract the business of customers desiring to keep all of their activities on the global grid unidentified.

Even if anonymous remailers are tolerated because they provide a useful service or are suffered because there is no meaningful mechanism for enforcing a prohibition against them, technological means for blocking messages from such servers still exist.\textsuperscript{154} Thus, recipients have some freedom of choice to refuse to accept such messages, as long as they can be identified as coming from an anonymous source that can be deflected. In the United States, no one has the right to inflict material upon an unwilling receiver, and nothing in the First Amendment contradicts this basic protection of the sanctity of personal space.\textsuperscript{155} Although the First Amendment protects individuals from infringement of speech by the government, it neither guarantees that such speech will be heard nor allows such speech to be delivered into a private space. Instead, the First Amendment's purpose is to provide public forums into which messages may be inserted without censorship. Nevertheless, this right to speak in a public forum does not guarantee the right to enter into space provided by a "publisher" when that publisher retains the right over entry into that space.\textsuperscript{156}

Furthermore, electronic coding of messages that will permit freedom of choice to deal with anonymous messages or that will refuse to deal with them should be devised. Guidelines should be refined so as to permit the use of aliases and pseudonyms in electronic playgrounds and to preserve the privilege of posting anonymous messages when doing so serves some useful public purpose like whistle-blowing. To preserve order and civility, however, abusive posters of anonymous messages must not be permitted to insulate themselves from accountability for their wrongdoing.

V. CONCLUSIONS

First Amendment lawyers should be wary of applying current legal metaphors to the newer electronic communication spaces without substantially immersing themselves in the experience of using such cyberspaces. Legislators

\textsuperscript{154} Network managers have devised "kill files" and "bozo filters" to screen out messages from offending sources. Although individual users may need greater computer competence than most now possess, systems could be designed to make these screening devices easy to deploy. Regulatory agencies or national legislation could require that electronic telecommunication providers design their software to facilitate such freedom of choice over unwanted messages. See ELECTRONIC FRONTIER FOUND., supra note 20, § 4.2 (explaining how kill files work and how to employ them).

\textsuperscript{155} See Rowan, 397 U.S. at 735–38.

\textsuperscript{156} The United States may find itself in a dilemma if the common carrier concept falls into disuse and electronic transport providers are not required to accept messages (as telephone networks and postal services are required to do today). If all electronic transport providers are also information providers and claim the censorship rights that have been granted other mass media, then no guaranteed right of access to the electronic media may exist. See, e.g., Nicholas Johnson, Jefferson on the Internet, 47 FED. COMM. L.J. 281, 285 (1994).
should be equally cautious.\textsuperscript{157} It is tempting and easy to say that the First Amendment is an absolute that requires a governmental "hands off" policy for all forms of communication and that the scarcity doctrine was a terrible mistake. As Judge David Bazelon, who presided over many appeals in communication cases, observed, we regulate broadcasting not because it is scarce but because it is the most powerful form of communication and methodology for manipulation of human behavior yet known to mankind.\textsuperscript{158}

There is no reason to believe that computer-mediated communication will be any less powerful a medium for the manipulation of human behavior, although it does seem to offer a proliferation of communication channels that carry the hope of genuine diversity and both personal and group autonomy. More choice and control in the hands of individual users seem assured, and lower transmission costs with faster delivery and greater scope of coverage seem reasonably attainable. Nonetheless, if we compare the "hype" with which cable television was offered to the public in the early 1970's with the duplication of programming sources and genres available on this multiplicity of channels today, there is much room for cynicism. Perhaps the Networld will not be the salvation of democracy and will not bring on the millennium for the First Amendment's promise of an uninhibited "marketplace of ideas."

The flow of information is not free financially, nor is it immune to other constraints. There are costs to building transmission systems, to buying equipment to access those systems, and to learning how to manipulate the software that makes it possible to engage in electronic discourse. There are also costs to finding the time to search for and download the information that is made available by sources prepared to underwrite their own costs of processing and uploading information. Not everyone will have the time, money, equipment, or skills to engage in a worldwide dialogue on the Networld of the future.

The media tend to spot and magnify the activities of miscreants, clowns, and fools in cyberspaces because they make good reading and viewing. The peccadillos of the few, however, should not be permitted to override the beneficial uses of these new computer-mediated communications systems. They are only a small portion of what is actually happening. Despite the problems of access and abuse, a thorough look through the magnifying glass will reveal

\textsuperscript{157} As one commentator remarked:

[T]he Internet is . . . a vehicle for mass social interaction with its own well-developed culture. Thus, to the extent that Congress attempts to impose further controls on the Net, such efforts run counter to the self-policing culture that has emerged in many quarters of cyberspace—it will have to do so with a fuller understanding both of the Internet's technical aspects and of its cultural norms.

Eckenwiler, supra note 142, at S32.

\textsuperscript{158} David L. Bazelon, FCC Regulation of the Telecommunications Press, 1975 DUKE L.J. 213, 220-23, 228. "[T]he problem is not scarcity of frequencies but rather the particularly powerful nature of TV communication." Id. at 228.
a seething hotbed of democratic discourse, public service data bases, and volunteers spending hours at their keyboards uploading the treasures of world literature so that anyone across the global grid may access them. Volunteers who compile the frequently asked questions (FAQs) are sharing their expertise willingly and without charge to help others become familiar with these new information superhighways. Indeed, the principles of the First Amendment are alive and well in many cybercommunities throughout the Networld.

Generic principles applied uniformly will not suffice to govern the information superhighways of the future, for the latter will be at least as rich and vast a technological landscape as the many media we see deployed today. The current legal landscape is complex and diverse. The finely honed principles developed to determine fair and equitable governance of the different technologies of communication, such as publishing, broadcasting, telecommunications, and cable, will not wither away with the merging of the media into a digital bitstream. Instead, these media themselves are evidence that the law needs to be refined to ensure access and equity in varying circumstances. The landlords of cyberspaces will be no more uniformly in agreement than the landlords of real spaces.

Computer-mediated communication is a diverse mix of electronic conferences, town meetings, bulletin boards, newsletters, radio talk shows, and almost any other variety of people-to-people communication that information entrepreneurs are likely to devise. Lawyers, litigants, legislators, judges, and juries will continue to look for appropriate metaphors and apply them to the cyberspaces—sometimes willy-nilly, sometimes more thoughtfully, and sometimes not at all. To the extent that they do so with an open mind and with actual exposure to the electronic commerce that they are trying to govern, the outcome of their efforts will become more acceptable and desirable.

The traffic on this grid will be global, not merely national. Thus, the First Amendment will be only one small way of prohibiting heavy-handed regulation by one national entity—the United States of America. Other nations may follow our lead, but the inability to ensure that such will be the case is no reason for reticence in putting forth our own views of how the cybercommunities should be governed. Current users of these spaces, however, have some very strong opinions about how they wish to develop the “virtual communities” they are building. They do not welcome intruders unacquainted with what they consider to be a promising frontier of new and exciting opportunities to build more open and diverse discourse among peoples of all races, colors, genders, and predilections. Cyberspaces are populated by people-to-people communication—including person-to-person, some-to-some, and many-to-many. Computer-mediated communication offers an environment unlike any heretofore made available, with the potential for genuinely interactive and cooperative innovation. To saddle such promise with an overload of baggage from a bygone era would be tragic.
Lawyers and their clients must be cautious in their approach to litigation. Judges and juries must forbear in casting the net of existing laws too wide. Legislators must be thoughtful in their approach to rigid statutory requirements. If a rich diversity of information resources is to be made available, and if a flourishing computer-mediated information marketplace is to be realized, users must be willing to devote time and patience to devise "netiquette" appropriate for their varying circumstances. Many are already doing so. These new cyberspaces offer a precious laboratory of law in gestation, developing largely without the aid of lawyers. As lawyers flock to their assistance, let us hope they do so with humility and with the understanding that the future need not necessarily follow the path of the past.