Cyberspace, the Free Market and the Free Marketplace of Ideas: Recognizing Legal Differences in Computer Bulletin Board Functions

Eric Goldman
Santa Clara University School of Law, egoldman@gmail.com

Follow this and additional works at: http://digitalcommons.law.scu.edu/facpubs

Part of the Law Commons

Recommended Citation
16 Hastings Comm. & Ent. L.J. 87

This Article is brought to you for free and open access by the Faculty Scholarship at Santa Clara Law Digital Commons. It has been accepted for inclusion in Faculty Publications by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.
Cyberspace, the Free Market and the 
Free Marketplace of Ideas: 
Recognizing Legal Differences in 
Computer Bulletin Board Functions

by
ERIC SCHLACHTER*

Table of Contents

I. Difficult Issues Resulting from Changing Technologies . . 89
   A. The Emergence of BBSs as a Communication Medium ............................................ 91
   B. The Need for a Law of Cyberspace ................ 97
   C. The Quest for the Appropriate Legal Analogy Applicable to Sysops .. 98

II. Breaking Down Computer Bulletin Board Systems Into Their Key Characteristics ................................ 101
   A. Who is the Sysop? ................................ 101
   B. The Sysop’s Control ................................ 106
   C. BBS Functions ...................................... 107
      1. Message Functions ............................... 107
      2. User/System Interaction and Information Services ........................................... 108
      3. “Gateways”........................................... 111

III. Analysis of the Implications of Various Legal Analogies as Applied to the BBS Context ................. 111

* M.B.A. 1994, UCLA; J.D. 1994, UCLA; B.A. 1988, UCLA. The author gratefully acknowledges the special contributions and assistance of John Brice, Esq., Mike Godwin, Esq., Sandra Goldstein Hirsh, Gail Schlachter, Marc Smith and Professor Tracy Westen. The author is especially appreciative of the thorough and competent work of the COMM/ENT editors and staff.

The author invites interested readers to initiate a cyberspace dialogue. He can be reached at his Internet address: eschlach@netcom.com. He also refers interested readers to a related article, entitled “Computer Bulletin Board Technology: Sysop Control and Liability in a Decentralized Information Economy,” in the conference proceedings for the International Symposium on Technology and Society 1993 (available from the Institute of Electrical and Electronics Engineers, Inc., IEEE Catalog Number 93CH3263-1, or the author).
A. Synopses of the Rights and Obligations Involved with Each Analogy ........................................ 111
  1. The Extent of Government Regulation ............. 112
  2. Owner’s Extent of Control/User’s Right to Access .............................................. 113
  3. Owner’s Liability for the Statements or Actions of Others ........................................ 116
B. State Actors and the Public Forum Doctrine ........ 119
C. Policy Considerations—The Merits of BBSs and Interest Balancing ..................................... 121

IV. Application of Existing Legal Doctrines to Specific BBS Functions ........................................ 129
A. First and Fourth Amendment Cross-Functional Constitutional Considerations ................................. 130
  1. Unreasonable Search and Seizure/Prior Restraint .................................................. 130
  2. Associational Interests .................................................. 131
B. Function-Specific Analogies ........................................ 133
  1. Message Posting .................................................. 135
  2. Electronic Mail .................................................. 139
  3. Real-Time Conferencing .......................................... 141
  4. Information Resources Dissemination ............. 142
  5. Software Distribution and Commercial Services 145
  6. Gateways .................................................. 146

V. Conclusions .................................................. 147
I

Difficult Issues Resulting from Changing Technologies

The digital revolution. Net surfing. Five hundred channels. Multimedia. Global village. Cyberspace.1 The information superhighway/information infrastructure. These and other buzzwords have proliferated in recent years, describing technology that promises to change our lives.

The past year has brought an explosion of joint ventures and mergers among various media and entertainment entities, computer companies, and telecommunications providers.2 These projects reflect

1. The phrase "cyberspace" was initially popularized by William Gibson in his 1984 book, NEUROMANCER. For a detailed look at Gibson's definition of cyberspace throughout his various novels, see David G.W. Birch & S. Peter Buck, What is Cyberspace?, available in Internet via gopher, gopher.eff.org.

The definition of cyberspace can be conceptually difficult and amorphous, reflecting the ethereal nature of the technology. However, a reasonably descriptive definition was posited by Michael Benedikt, chair of University of Texas at Austin's Department of Architecture:

Cyberspace is a globally networked, computer-sustained, computer-accessed, and computer-generated, multi-dimensional, artificial, or "virtual" reality. In this world, onto which every computer screen is a window, actual, geographic distance is irrelevant. Objects seen or heard are neither physical nor, necessarily, presentations of physical objects, but are rather—in form, character, and action—made up of data, of pure information. This information is derived in part from the operation of the natural, physical world, but is derived primarily from the immense traffic of symbolic information, images, sounds, and people, that constitute human enterprise in science, art, business, and culture.


The cyberspace analogy is based on the fact that most physical space actions have electronic space (i.e., cyberspace) equivalents. See Jack Rickard, Preface to the Second Edition of LANCE ROSE & JONATHAN WALLACE, SYSLAW at xiii (2d ed. 1992) ("At an increasing pace, real world transactions are being 'translated' into online analogs."); John Arnold, The Medium is Messages, MIAMI HERALD, Sept. 28, 1985, at 1D ("[BBSs] contain the equivalent of want ads and graffiti, reminders and requests, jokes and personal messages."); cf. Pair Weds Via Computer Link, S.F. EXAMINER, Nov. 14, 1993, at A12 (describing an on-line wedding between a couple that also met on-line).

2. See, e.g., Lawrence M. Fisher, News Corp. Buys On-Line Network, N.Y. TIMES, Sept. 2, 1993, at D4 (reporting that News Corp. purchased Delphi BBS as a way to expand its distribution channels); William Glaberson, Times Mirror to Go On-Line Through Prodigy, S.F. CHRON., Aug. 5, 1993, at D1 (explaining Prodigy's arrangement with the Times Mirror Co. and Cox Newspapers to offer their newspapers' contents, plus background and source material, on-line); Carla Lazzareschi, The Scramble Is on to Find New Partners—Or Be Left in the Dust, L.A. TIMES, Oct. 14, 1993, at D1 (describing how the merger between Bell Atlantic Corp. and Tele-Communications, Inc. set off soul searching by phone companies and cable companies over the need for alliances); Cindy Skrzycki & Paul Fahri, The Multimedia Feeding Frenzy: As Technology Converges, So Are Communications Giants Looking for Deals—and Billions in Future Profits, WASH. POST, May 23, 1993, at H1 (listing numerous deals, including U.S. West telephone company's $2.5 billion investment in Time Warner, Southwestern Bell's $650 million purchase of Virginia cable television systems, and a joint venture between Microsoft, Intel Corp., and General Instrument Corp. to
the increasing convergence of computers, communications, and the media.

Computer bulletin board systems (BBSs) represent a key technology at the intersection of these disciplines, occupying an increasingly important role in today's mass communications. A BBS is an electronic network of computers. At the heart of the BBS is the central computer, set up and operated by the system operator (commonly called the "sysop"). Users link their computers to the central BBS computer by modem. Once users have accessed the BBS, they may communicate with other users, obtain information from databases, obtain software, or perform other activities.

3. To avoid confusion, this Essay uses the term "computer bulletin board system" generically to include computer bulletin boards, electronic bulletin boards, network nodes, on-line services, information services, electronic information services, videotext services, electronic publishers, electronic mail systems, and electronic networks. This Essay integrates the legal analysis applied to these entities because current technology and usage indicate that each of these electronic communication methods performs essentially the same functions (or, that the distinctions in the functions performed are not legally significant). See Philip L. Becker et al., Introduction to PC Communications 76 (1992) [hereinafter Becker, PC Communications].

4. "[T]he BBS has become the most common form of mass communication in the country." T.R. Reid, Mass Communicate Your Messages at Little Cost, WASH. POST, Dec. 2, 1991, at F18 [hereinafter Reid, Mass Communicate].

5. For a description of some of the computer hardware requirements of BBSs, see Loftus E. Becker, Jr., The Liability of Computer Bulletin Board Operators for Defamation Posted by Others, 22 CONNECT. L. REV. 203, 207-08 (1989) [hereinafter Becker, Bulletin Board Operators].

6. Douglas C. McGill, Newest City Meeting Places are in Computers, N.Y. TIMES, Mar. 21, 1984, at B1. Sysops range from individuals to large corporations to government entities. See infra part II.A. In general, this Essay does not distinguish between BBS owners, sysops, and system administrators. Where BBS owners have retained sysops as independent contractors (see infra note 307), this Essay's analysis applies only to the sysop.


8. See infra part II.C.
RECOGNIZING LEGAL DIFFERENCES IN BBSs

A. The Emergence of BBSs as a Communication Medium

Over the past fifteen years, BBS usage has grown exponentially. The United States has as many as 60,000 public and commercial BBSs, 120,000 private and corporate BBSs, and ten million users. This popularity can be primarily attributed to two factors. First, BBSs are inexpensive to set up and use. This makes them one of the lowest cost mass media. Second, because users retain some anonymity or because of the ease and power of BBS communication, users...

9. The first BBS was established in 1978 when a computer enthusiast transferred the physical contents of his computer club’s bulletin board onto his computer and made the electronic files accessible to other club members. Becker, PC Communications, supra note 3, at 73-74; see also Janet L. Balas, Bulletin Board Systems: A Nostalgic Look Back, Computers in Libr., May 1993, at 24 (elaborating on the history).


12. Id.


14. Membership in a commercial BBS costs as little as $15 annually, and there are many free BBSs. See infra notes 61, 64-65 and accompanying text.

15. “[BBSs are] the lowest entry-barrier mass-communication system in history. . . . [A]nybody can come up with the capital needed to start a bulletin board.” Reid, Mass Communicate, supra note 4, at F18 (quoting Ralph Nader); see also Freedom and the New Age, L.A. Times, Nov. 27, 1985, at B4 (“[BBSs] are the vanguard of the democratization of communication. . . .”).

The low cost of entry into the BBS industry has significant implications for the perception that media access depends on media ownership. See infra text accompanying notes 214-17.

16. There are two types of anonymity: (1) complete anonymity, such as that gained by the use of passwords or code names, and (2) social anonymity, where there is a minimal chance of physical contact or subsequent significant interaction. While many BBSs previously allowed users to access their BBS using only code names, so that users had complete anonymity (see Beall, supra note 13, at 512 n.100), most BBSs now deny complete anonymity by requiring users to register their names and phone numbers accurately. Becker, PC Communications, supra note 3, at 333. But see William M. Bulkeley, Censorship Fights Heat up on Academic Networks, WALL ST. J., May 24, 1993, at B1, B6 (explaining that some BBSs “strip” users’ names before sending messages to other BBSs). However, users who do not have absolute anonymity often retain social anonymity. See Terri A. Cutrera, Computer Networks, Libel and the First Amendment, 11 COMPUTER/L.J. 555, 557, 559-60 (1992) [hereinafter Cutrera, Computer Networks] (describing how social anonymity can result in misunderstandings); Martin Lasden, Of Bytes and Bulletin Boards, N.Y. Times, Aug. 4, 1985, § 6, at 34, 36 (noting that, unlike the typical exchange of letters between persons known to each other, “familiarity is the exception rather than the rule” in BBS communication).

Anonymity allows users to adopt new personas. John Markoff, The Latest Technology Fuels the Oldest of Drivers, N.Y. Times, Mar. 22, 1992, § 4, at 5 [hereinafter Markoff, The...
may lower their psychological barriers and "open up, connecting [them] even more intimately to others in society." As a result of these and other factors, BBSs have taken a place alongside "traditional" media as a major force for intellectual, political, and informational exchanges. For example, during global crises, BBS communication has become an important source of news infor-

Latest Technology] (noting that a user may assume a different identity, role, gender, and age). While this freedom may allow timid users to find new avenues of expression, it can also result in gender-bending or mythical experiences. See, e.g., Michael Schrage, Forget the Message, The Medium is a Mask, L.A. TIMES, June 7, 1990, at D1 (describing men who have signed on-line as women).  

17. See Gina M. Garramone et al., Uses of Political Bulletin Boards, 30 J. of Broadcasting & Electronic Media 325, 329 (1986); see also Arnold, supra note 1, at 3D ("[It allows people to sound off.") (quoting Bob Sherman, sysop of The Big Apple BBS); Robert O'Harrow, Jr., Computer-Friendly Homes Increasing: Electronic Bulletin Boards Provide Many Residents with Comfort, Communication, WASH. POST, Dec. 27, 1992, at B1 (quoting one user as describing how BBSs have "almost a confessional atmosphere"); Janny Scott, On-Line, and Maybe Out of Line, L.A. TIMES, Sept. 24, 1993, at A1 (explaining that on-line communication tends to be intimate, democratic, and playful, but because of the "disinhibition" of the medium, it can also be blunt, extreme and impulsive).  


However, this freedom of intimacy carries some implicit responsibilities: The Dial-Your-Match BBS reminds users that "[j]ust as it is not acceptable to walk up to a stranger and describe your sexual desires in graphic detail, it is not correct here." For Every Taste, a Bulletin Board, U.S. NEWS & WORLD REP., June 3, 1985, at 59 [hereinafter For Every Taste]; cf. BECKER, PC COMMUNICATIONS, supra note 3, at 334 ("Most BBS etiquette is just common sense and follows the same rules as any social interaction."); Marc Silver, Action on the Boards, U.S. NEWS & WORLD REP., Nov. 18, 1991, at 96 (explaining that rule number one of an eight-rule etiquette guide for BBS users is "[t]here aren't many rules, so don't break them").  

mation. BBSs also support political expression, creating new ways for politicians to receive feedback from their constituents and increasing citizens’ opportunities to discuss and debate issues. For example, when one Colorado sysop, concerned about a proposed but unpublicized city ordinance, typed the ordinance’s text into his BBS, 175 people showed up at the next city council meeting to express their opinions on the ordinance.

However, as with any emerging technology, users have also exploited the technology’s dark side. Because BBSs are tremendously powerful tools for communication, they empower individuals to engage in socially-undesirable speech or anti-social behavior. There are a number of ways that BBSs can support illegal activity, such as through the illegal distribution of telephone card numbers or copying information.


21. See Garramone et al., supra note 17, at 326; Lawrence J. Magid, White House is Definitely Plugged in, L.A. TIMES, Mar. 19, 1993, at D3 (describing how the White House and Congress can be reached through electronic mail and how constituents can increase their political involvement and awareness through electronic resources); Pitta, supra note 18, at 132 (explaining that many of the messages U.S. Representative Mel Levine received on Santa Monica’s public electronic network were from constituents who would not otherwise participate in the political process).

22. See Garramone et al., supra note 17, at 326; see also Katsh, The First Amendment and Technological Change, supra note 18, at 1482-83 (noting that BBSs allow for more rapid expression of political grievances and concerns); Browning, supra note 20, at 1624 (“Computer-to-computer communications . . . are revolutionizing the way Americans interact with their government.”); Mitchell Kapor, Civil Liberties in Cyberspace: Computers, Networks and Public Policy, SCI. AM., Sept. 1991, at 158, 160 (“[C]omputer-based bulletin boards and conferencing systems support some of the most vigorous exercise of the First Amendment freedoms of expression and association that this country has ever seen.”).


24. For example, in 1984, sysop Thomas Tcimpidis was arrested because a user had posted stolen telephone credit card numbers on Tcimpidis’s BBS without his knowledge. Lynn Becker, Electronic Publishing: First Amendment Issues in the Twenty-First Century, 13 FORDHAM URB. L.J. 801, 801-06 (1985) [hereinafter Becker, Electronic Publishing]; Kim Uyehara, Computer Bulletin Boards: Let the Operator Beware, STUDENT LAW., Apr. 1986, at 28, 30. Telephone credit cards have played a significant role in BBSs because users must pay toll charges for the time they are logged on to the BBS. See Beall, supra note 13, at 501; cf. Berck, supra note 10, at 12 (noting that at least one telephone company includes a list of BBSs in its phone bills as a way of encouraging use and generating additional reve-
righted software. BBSs also are used to propagate harmful speech such as defamation, child pornography, hate speech and anti-Semitism, and to facilitate hate crimes and copyright infringement.

As a result, some users have sought ways to avoid paying telephone charges while accessing BBSs nationwide. See generally Soma et al., supra note 10, at 573-74 (describing some of the ways that "phreakers," people who play with the telephone system, attempt to avoid long-distance telephone charges).


25. See Lasden, supra note 16, at 42 (suggesting that, in 1983, almost half of the BBSs traded "pirated" copyrighted software).


27. In 1991, an America Online user complained that he received digitized photos of child pornography sent to his private electronic mailbox. Jim Doyle, FBI Probing Child Porn on Computers: Fremont Man Complains of Illicit Electronic Mail, S.F. CHRON., Dec. 5, 1991, at A23. America Online said that, because the photos were transmitted as a private communication, it had no knowledge of the transmissions. Id.


28. In 1988, Stanford University cancelled its subscription to a USENET discussion forum that contained racist jokes. After a computer science professor made the forum available on his own computer, the University changed its decision. See W. John Moore, Taming Cyberspace, 24 NAT'L. J. 745, 748 (1992) [hereinafter Moore, Taming Cyberspace]; see also Bill Workman, Unplugging Racist Jokes Starts Furor at Stanford, S.F. CHRON., Feb. 1, 1989, at A4.

In 1991, the Anti-Defamation League of B'nai B'rith criticized Prodigy for allowing anti-Semitic messages to be sent on the system. It was later shown that the worst messages had been sent as private electronic mail, which Prodigy transmits without reading, and Prodigy's censors had repeatedly rejected these messages for public posting as offensive. Barnaby J. Feder, Towards Defining Free Speech in the Computer Age, N.Y. TIMES, Nov. 3,
The power of this new technology has caused some private and state actors to respond aggressively, overreacting to weak threats and inhibiting legitimate conduct.  

Ambiguities arise as old law is applied to new technologies. With the inherent ambiguities of cyberspace, the need to define its boundaries for legal purposes becomes even more critical. For example, the boundaries on permissible Fourth Amendment searches and seizures can be murky even in physical space. The absence of such boundaries in cyberspace can result in searches far beyond the necessary scope.


29. The Aryan Brotherhood Youth Movement reportedly used the Liberty BBS network to compile a list of homosexuals as potential targets of hate crimes. Jackson, supra note 27, at A20.


31. The 1990 raid of Steve Jackson Games, Inc. is a well-known example of government's aggressive approach. In response to their belief that a company employee was a hacker who kept his documents on the company BBS, Secret Service agents seized the company's computer, files, and disks that were being used to write a role playing game. Michael Alexander, Suit Seeks to Define User Rights, COMPUTERWORLD, May 6, 1991, at 1, 4. See generally John Perry Barlow, Crime and Puzzlement, WHOLE EARTH REV., Fall 1990, at 44, 51-52 (describing the story); Kapor, supra note 22, at 158-60 (enumerating the errors made by the Secret Service in dealing with Steve Jackson). As a result of the seizure, the company lost $125,000 in revenue, had to lay off eight employees, and delayed publication of a book for six weeks. Alexander, supra, at 4. Admonishing the Secret Service for its "sloppiness," a federal district court judge awarded Steve Jackson Games $8781 in expenses and $42,259 in lost revenue under the Privacy Protection Act, and $1000 per plaintiff under the Electronic Communications Privacy Act. Steve Jackson Games, Inc. v. Secret Serv., 816 F. Supp. 432 (W.D. Tex. 1993).

Another prominent incident involved Craig Neidorf, who distributed an electronic newsletter called Phrack over his BBS. Government officials prosecuted Neidorf for publishing in Phrack a telephone company document regarding the emergency 911 system that, allegedly, had been stolen. See, e.g., United States v. Riggs, 743 F. Supp. 556, 558-59 (N.D. Ill. 1990); United States v. Riggs, 739 F. Supp. 414, 416-18 (N.D. Ill. 1990). The case was dropped when evidence was introduced that the same document, allegedly worth $79,449, was publicly available for sale for $13. Joshua Quittner, Computer Rights: Advocates Worry About Overzealousness in the Crackdown on Hackers, NEWSDAY, Sept. 4, 1990, at 1. See generally Barlow, supra, at 49-51.
For example, in Operation Sun Devil, when government agents seized BBS computers, they searched *entire* hard drives, reading private electronic mail ("e-mail") not associated with the crimes alleged on the search warrants.\(^{32}\)

Furthermore, while the technology has empowered users and induced a strong response from government, it has also empowered sysops to control the flow of information. For example, Prodigy, a large commercial BBS, has censored users for various reasons. Prodigy has prohibited users from posting public messages critical of Prodigy and ultimately ejected some users who failed to comply.\(^{33}\) Prodigy has also regularly edited and refused to post submissions.\(^{34}\)

\(^{32}\) See, e.g., Jim Sulski, *Crackdown on Crime is Raising Question of Computer Rights*, CHI. TRIB., Nov. 18, 1990, at C17. See generally Barlow, *supra* note 31, at 48-52 (describing Operation Sun Devil, in particular how police used tactics such as forcible entry with guns drawn in situations which seemingly did not require such shows of force).

\(^{33}\) The incident began when Prodigy instituted a charge (in addition to its regular monthly fee) of 25 cents for every electronic letter over 30 per month. Marianne Taylor, *Users Say Computer Network is Muzzling Their Give-and-Take*, CHI. TRIB., Jan. 7, 1991, at C1. Prodigy stated its actions were based on the fact that its e-mail volume was increasing by 20% *each month*. John Markoff, *Home-Computer Network Criticized for Limiting Users*, N.Y. TIMES, Nov. 27, 1990, at D1, D5 [hereinafter Markoff, *Home-Computer Network*]. Outraged users sent electronic complaint letters to other users and to the companies that advertised on Prodigy. Prodigy responded by cancelling the subscriptions of 12 of the worst complainers, although after intervention by the ACLU, these subscribers were invited back as long as they agreed to some guidelines. Michael R. Zimmerman, *Prodigy Offers Olive Branch, of Sorts, to Protesting Users*, PC WEEK, Dec. 3, 1990, at 13. See generally Di Lello, *supra* note 28, at 207-08 (describing the incident).

\(^{34}\) In a letter to the *New York Times*, Prodigy's director of market programs and communications gave some examples of submissions that Prodigy chose not to publish:

- "I'm thinking of killing myself. Which is less painful: hanging or slashing my wrists?"
- "My neighbor, William, embezzled $10,000 from his company and is still stealing to this day."
- "Little girls in tight jeans and T-shirts are a real turn-on to guys like me. Write to me at P.O. Box . . . ."
- "Here's how to avoid paying for HBO: Climb the telephone pole outside your house and . . . ."
- "You can't get pregnant if you don't have an orgasm."


While Prodigy's decision not to publish those submissions may not be especially controversial, Prodigy came under fire for cancelling the "Health Spa" discussion forum in 1989, which began as a forum for discussing gay sexual practices but developed into a heated debate between religious fundamentalists and gays. See Moore, *Taming Cyberspace*, *supra* note 28, at 748. Users have also complained about Prodigy's refusal to post messages using the term "death certificate" or questioning the Catholic church's stand on birth control in the context of a debate about abortion. Chris Reidy, *Computer Flap: Is Speech Free on Prodigy?*, BOSTON GLOBE, Jan. 30, 1991, at 35. Apparently, fewer users were upset when Prodigy cancelled its "Frank Discussion" forum, which was intended to support discussion on alternative lifestyles but occasionally degenerated into explicit and
B. The Need for a Law of Cyberspace

Presently, there is significant uncertainty regarding which laws govern the situations described above and how those laws will be applied. Although laws have begun to address primary criminal and civil liability, the extent of vicarious sysop liability for users' actions remains undetermined. One reason sysop liability is tricky is that communication on BBSs presents a unique set of interests to balance. More significantly, however, the Constitution "tends to carve up the social, legal, and political universe along the lines of 'physical place' or 'temporal proximity.'" As a result, "[w]hen the lines along which our Constitution is drawn warp or vanish, what happens to the Constitution itself?"

Without physical or temporal boundaries, both substantive and procedural legal issues such as jurisdiction, choice of law, and enforcement are problematic.

35. For further discussion of the policy considerations in the BBS industry, see infra part III.C.


37. Id.

38. See Anne W. Branscomb, Common Law for the Electronic Frontier, SCI. AM., Sept. 1991, at 154, 158; see also Lance Rose, The Boy Who Cried Wolfenstein, BOARDWATCH MAG., Sept. 1992 (describing how CompuServe and other United States BBSs removed a game containing Nazi imagery for fear that German residents would obtain a copy in violation of German laws); It's New, It's Hard to Track Down and There Are No Legal Precedents, VANCOUVER SUN, Sept. 12, 1992, at A4 (reporting that Canadian officials are having difficulty enforcing a law against material depicting child pornography, sexual violence, or sexual degradation because much of this material is digitized in the United States and sent electronically to Canadian BBSs). See generally Di Lello, supra note 28, at 234-39 (analyzing choice of law issues in a hypothetical class action suit against Prodigy); John D.
As future legislation and court rulings address BBSs' unique aspects and as BBS technology proliferates, legislators and jurists will find it increasingly appropriate to discuss the law of cyberspace, the electronic version of physical space. As the courts and legislatures start mapping the contours of law in cyberspace, the powers of the cyberspace media and its keepers (the sysops) will create numerous questions of constitutional and tort jurisprudence. How should the bundle of individual constitutional rights contained in the Bill of Rights be protected from government infringement in cyberspace? How extensively should the government regulate private sysop conduct? Should the government prohibit private actors from determining the types of conversations or activities that take place on private BBSs, or who can gain access? What combination of direct regulation and tort liability will provide a socially desirable level of control over private BBS owners? How can we as a society strike a satisfactory balance between private autonomy and appropriate government intervention?

C. The Quest for the Appropriate Legal Analogy Applicable to Sysops

Unfortunately, the law has difficulty adapting to major advancements in communications technology. This is particularly true in the case of BBS technology, in which the traditional legal trifurcation of print, broadcasting, and common carriage is collapsed into one me-


39. One commentator has estimated, perhaps hyperbolically, that the United States will have one million BBSs by the year 2000. See Becker, *PC Communications*, supra note 3, at 341. In any case, at some point the ubiquity and importance of computer-based communication may radically alter current communication dynamics. See Michael L. Taviss, Editorial Comment, *Dueling Forums: The Public Forum Doctrine's Failure to Protect the Electronic Forum*, 60 U. CIN. L. REV. 757, 788-89 (1992) (suggesting that BBSs may play a "major, if not decisive, role in disseminating expression" and could make alternative modes of communication "scarce or impractical"); O'Harrow, * supra* note 17, at B1 ("'Things are now reaching a threshold . . . [BBSs are] being positioned, I guess, to permeate every part of society.'") (quoting Fred Wood of the Office of Technology Assessment); see also infra part V.


41. See Pool, * supra* note 18, at 7 (noting the inherent difficulties of analogizing new technology to existing legal precedents); Laurence H. Tribe, *American Constitutional Law* 1007 (2d ed. 1988) [hereinafter Tribe, *American Constitutional Law*] ("The rate of technological change has outstripped the ability of the law, lurching from one precedent to another, to address new realities.").
However, the uniqueness of BBSs does not mean that new legal rules must be fashioned to govern sysops' legal rights and responsibilities; rather, the proper application of existing legal rules will reach satisfactory legal results without judicial activism or legislative intervention.

Commentators on BBS legal issues have sought to apply existing legal doctrine to sysops from the very beginning. Sysops have been analogized to:

- newspaper publishers and editors;
- "secondary publishers," such as libraries and booksellers;
- broadcast media, such as radio or television;
- common carriers, such as telephones and postal mail; and
- private real property owners.

However, most commentators have proposed these analogies to solve single legal problems, without considering how these analogies apply to other problems that will inevitably arise on BBSs. Unfortunately,

---

42. See Katsh, The First Amendment and Technological Change, supra note 18, at 1480-81 (explaining how electronic information processing has blurred the traditional lines between First Amendment "boxes"); McDaniel, supra note 7, at 784 ("Videotext is many types of services bundled together."); cf. Kevin M. Savetz, Plug in, Log on, Tune in, MICROTIMES, May 31, 1993, at 154 (describing the distribution of an electronic talk "radio" program, complete with advertising sponsors, through the Internet).

As a result, BBS technology may transcend the trifurcation and warrant a new legal approach. See Taviss, supra note 39, at 789 ("Eventually, computer-based expression may require a... drastic break with First Amendment tradition, and the courts and legislatures may have to craft completely new laws to protect it.") (footnote omitted); Tribe, The Constitution in Cyberspace, supra note 36, at 17 ("The Constitution's architecture can easily come to seem quaintly irrelevant—or at least impossible to take very seriously—in the world as reconstituted by the microchip.").

43. To illustrate the adequacy of existing law if interpreted correctly, Laurence Tribe has proposed a Twenty-Seventh Amendment:

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

Tribe, The Constitution in Cyberspace, supra note 36, at 39; see Freedom and the New Age, supra note 15, at B4 ("The Constitution protects electronic words as much as spoken or written ones... Whatever is legal to publish on paper should also be legal to publish electronically."); see also POOL, supra note 18, at 246; McDaniel, supra note 7. See generally Jim Warren, Guaranteeing Constitutional Freedoms into the 21st Century, MICROTIMES, Mar. 2, 1992, at 26, 26 (suggesting applications of Tribe's proposed amendment in various legal situations).

44. This law-by-analogy approach is not new. See POOL, supra note 18, at 103 (noting how courts applied the law of railroads to telegraphy because telegraphy was seen as the successor to railroads and the law of telegraphy was applied to telephones for the same reason).
the "law of unintended consequences" applies: In trying to solve an isolated problem, the "solution" creates other problems. For example, many commentators have argued, and continue to argue, that to protect BBSs from prior restraints effected by BBS seizures, sysops should be analogized to print publishers. On the other hand, Prodigy has been repeatedly criticized for claiming it has editorial control similar to that of print publishers which allows it to discriminate on the basis of content and deny access to users.

The complexity and versatility of BBSs suggest that no single legal model or analogy will prove satisfactory. Consequently, some have argued for the development of a hybrid model. This Essay proposes a hybrid model that combines specific pieces of existing jurisprudence, each based on an appropriate analogy for a particular BBS function. To do so, this Essay breaks down the entity "computer bulletin board" into three categories that will serve as the building blocks for synthesizing the law of cyberspace from existing legal rules:

1. the identity of the owner/sysop;
2. the sysop's knowledge of, and control over, users' actions; and
3. the way the BBS is being used.

---


46. See, e.g., Kapor, supra note 22, at 162.

47. See Becker, Bulletin Board Operators, supra note 5, at 206 ("[I]t is a mistake to turn the legal rules on whether or not an entity is called a computer bulletin board . . . . We should not be misled by a label into thinking that all communication through computer bulletin boards is the same."); Ethan Katsh, Law in a Digital World: Computer Networks and Cyberspace, 38 VILL. L. REV. 403 (1993) [hereinafter Katsh, Law in a Digital World] (noting how the terms used for analogies often seem antiquated as the technology evolves); Naughton, supra note 19, at 412-13 (focusing only on the public messaging function "[i]n order to offer a coherent analogy"); Anthony J. Sassan, Note, Cubby, Inc. v. CompuServe, Inc.: Comparing Apples to Oranges: The Need for a New Media Classification, 5 SOFTWARE L.J. 821, 833 (1992); cf. Mark S. Nadel, A Technology Transparent Theory of the First Amendment and Access to Communications Media, 43 FED. COMM. L.J. 157 (1991) (arguing for new access rules that are based on the economic accessibility of the media rather than on "historical categories").

48. One distinction is whether the BBS is owned and operated by public or private entities. See infra part II.A.

49. See infra part II.B.

50. Uses include posting public messages, sending private e-mail, and accessing information databases. See infra part II.C.
Ultimately, all three characteristics are essential to tailoring existing legal doctrine to fit the myriad of legal difficulties that arise on BBSs.

Part II of this Essay addresses the current state of the BBS industry with respect to each of the three dimensions, illustrating the diversity of BBSs and sysops. Part III summarizes the jurisprudence that has developed for each of the relevant legal analogies proposed. Part III of the Essay demonstrates how legal rights and responsibilities vary with the amount of editorial control available to and exercised by the entities' owners. Part IV then methodically applies the conclusions of part III, developing the law of cyberspace by outlining appropriate analogies for each function. Significantly, part IV shows that sysops can and should have the choice to determine the amount of editorial control they exercise and the concomitant bundle of legal rights and responsibilities. Finally, part V concludes by discussing the interaction between the freedom to contract and the marketplace of ideas, arguing that a policy of permitting sysops to choose their bundle of rights and responsibilities, combined with a properly functioning market, will foster the free marketplace of ideas.

II

Breaking Down Computer Bulletin Board Systems Into Their Key Characteristics

This part separates computer bulletin board systems into three significant components: BBS ownership, sysop control, and BBS functions. The analysis will prove useful as this Essay reconstructs the BBS industry along various dimensions to develop appropriate legal doctrine.

A. Who Is the Sysop?

BBSs may be categorized as national and regional commercial BBSs, public and private free BBSs, corporate BBSs, and state-owned BBSs. Wide area electronic networks link BBSs and warrant special mention.

Some commercial BBSs have taken a "mass market" approach, developing a national user base and providing a comprehensive set of functions. For example, one large commercial BBS, Prodigy, is a joint venture of Sears Roebuck & Co. and International Business Machines Corporation\(^5\) and has approximately one million subscribers.\(^6\) Prodi-

---

5. BECKER, PC COMMUNICATIONS, supra note 3, at 259.
igi distinguishes itself from other commercial BBSs in three ways: (1) by promoting an on-line "family" atmosphere;\(^53\) (2) by routinely removing messages that do not meet its subjective standards;\(^54\) and (3) by displaying advertising on virtually every computer screen.\(^55\)

Other national commercial BBSs include GEnie,\(^56\) America Online,\(^57\) and CompuServe, which has 1.4 million subscribers\(^58\) and is the oldest\(^59\) commercial BBS. Although these BBSs have segmented the market somewhat, there is significant competition among them, especially based on pricing.\(^60\)

In addition to the handful of national commercial BBSs, there are many regional commercial BBSs.\(^61\) A typical regional BBS is the Channel 1 BBS in Cambridge, Massachusetts. Channel 1 has 250 forums and over four gigabytes of downloadable files, uses eighty-five

---

53. Prodigy claims to be the "Disney Channel" of BBSs. Moore, Ist Amendment, supra note 34, at 13.

54. Because Prodigy receives 175,000 postings a day, it has an automated screening process. Harmon, New Legal Frontier, supra note 26, at A24. First, Prodigy's computer scans each message for any of several dozen obscene or offensive words or phrases, and then Prodigy's screeners review flagged messages. Sandra Sugawara, Computer Networks and the First Amendment, Wash. Post, Oct. 26, 1991, at A12. The subjectivity of this process is reflected in the fact that at least one user would resubmit rejected messages until they were accepted by Prodigy. Adam Gaffin, Prodigy: Where Is It Going?, 1991, available in Internet via gopher, gopher.eff.org.

Because uploaded software is even more difficult to screen, Prodigy does not allow users to exchange software. See Becker, PC Communications, supra note 3, at 201.


56. GEnie is owned by General Electric Information Services and has 400,000 subscribers. See Laurie Flynn, Solving the On-Linear Equation, San Jose Mercury News, Jan. 17, 1993, at 1F.


58. Growth Off, supra note 52, at F17.

59. CompuServe was founded in 1979. Flynn, supra note 56, at 1F. CompuServe is owned by H&R Block Inc. Potts, supra note 57, at F1.

60. In comparing commercial BBSs, users must evaluate a complicated fee structure. There are at least six types of fees: set-up charges, monthly fees, hourly connect time charges based on the service accessed or the time of day, user volume charges, hourly charges based on the speed of the user's modem, and hourly communications surcharges based on long distance telephone access. The lack of standardized pricing makes cost comparison between BBSs very difficult. See generally Amy Harmon, Price War Erupts Among On-Line Computer Services, L.A. Times, Apr. 21, 1993, at D1 [hereinafter Harmon, Price War] (describing recent changes in national BBS pricing structures).

61. Regional commercial BBSs charge annual fees of $15 or more. Berck, supra note 10, at 12. The term "regional" is a partial misnomer since these BBSs can have a national user base. However, it suggests the smaller scale of these BBSs.
telephone lines, receives 2500 calls a day, and has annual revenues of $250,000.62 One of the most prominent regional BBSs, and a frequent trendsetter for the industry, is the Sausalito, California-based WELL (Whole Earth 'Lectronic Link), which has 6000 subscribers.63

Supplementing the commercial BBSs are the free BBSs, which constitute a major portion of the overall BBS industry.64 With the appropriate computer hardware, telephone lines, and software, anyone can set up a free public BBS. Sysops establish BBSs to serve the community,65 support discussion of a topic of interest,66 or just for fun.67 Private free BBSs are similar to public BBSs, except that access is restricted, often to people known to the sysop.68

BBSs set up for corporation- or organization-specific purposes are yet another segment of the BBS industry. The flexibility of BBS technology has supported numerous organizational uses. BBS tech-

62. Id; see also A ‘Poor Man’s CompuServe’ Can Put Cash in Your Pocket, PC/COMPUTING, Mar. 1991, at 286.
64. The exact percentage is hard to pin down. Compare Berck, supra note 10, at 12 (over one-third of all BBSs do not charge an access fee) with Becker, Bulletin Board Operators, supra note 5, at 227 n.119 (in 1989, “the majority of bulletin boards [were] not commercial operations”) and Feder, supra note 28, at 5 (in 1991, 90% of BBSs were not commercial). Free BBSs are also occasionally referred to as “hobby BBSs.” See BECKER, PC COMMUNICATIONS, supra note 3, at 325.
65. See For Every Taste, supra note 18, at 59 (explaining that Tom Mack, sysop for the Second Ring BBS, runs the BBS as a public service because he feels he should “give something back for all the things I’ve gotten”).
66. Some non-profit entities establish free BBSs to extend their reach into the community. Steve Snow, Join the Community, SAN JOSE MERCURY NEWS, June 20, 1993, at 1F. One of these BBSs, the Cleveland Free-Net, has 30,000 users and costs the sponsoring organizations upwards of $100,000 to start and $100,000 annually to maintain. Id. at 5F.
67. See Taviss, supra note 39, at 766 (explaining how sysops normally set up BBSs related to their interests).
68. Some BBSs have both public and private sections; general users may have limited access to BBS functions, while users known to the sysop will be given additional access. Jensen, supra note 18, at 221; see Manuel Schiffres, The Shadowy World of Computer 'Hackers', U.S. NEWS & WORLD REP., June 3, 1985, at 58, 59 (describing the private Off the Wall BBS, where the first level contains innocuous material, the second level supports discussions on software trading and X-rated material, and the final level provides illegal passwords and access codes). See generally Soma et al., supra note 10, at 572 n.3 (explaining that it is difficult to obtain an accurate count of the number of BBSs, since many are private).
nology can integrate a company through electronic mail systems for employees or through centralized information databases. Companies can also use BBSs as twenty-four-hour customer service lines or to facilitate the exchange of messages and documents between clients and the company. BBSs have also begun to play a special role in “making markets” by facilitating the connections of buyers and sellers.

In addition to the proliferation of BBSs throughout the private sector, government has found uses for BBSs at the federal, state, and local levels. For example, Blue Cross and Blue Shield use a BBS to collect, process, and submit Medicaid claims to the government. Berck, supra note 10, at 12. Nikon Precision Inc. uses a BBS to transmit information between corporate headquarters and 12 satellite offices, id., while some franchising companies use BBSs to collect information from franchise locations and to manage inventory and resources. Becker, PC Communications, supra note 3, at 75. Argus Chemical uses the Internet instead of Federal Express to distribute research reports company-wide, while Unocal disseminates maps and land surveys to all of its international offices through the Internet. Carla Lazzareschi, Wired: Businesses Create Cyber-space Land Rush on the Internet, L.A. TIMES, Aug. 22, 1993, at D1 [hereinafter Lazzareschi, Wired].

70. Berck, supra note 10, at 12; see John Eckhouse, Internet: The Information Superhighway Goes Commercial, S.F. CHRON., June 1, 1993, at C1, C7 (explaining how Apple Computer provides technical support over the Internet); Chris Oakes, The Internet: What It Is, How You Can Access It, & What It Can Do For You, COMPUTER CURRENTS, July 20, 1993, at 30, 33 (describing that many companies now provide product support through the Internet).


72. See Paul McCarthy, Going Once: Computer Technology Puts Art on the Auction Block, OMNI, Sept. 1993, at 18 (observing how art buyers can now purchase art on various BBSs); Thomas A. Stewart, Boom Time on the New Frontier, FORTUNE, Autumn 1993, at 153 (describing how a New York-based medical products company used a BBS to find a Chinese supplier).

73. See, e.g., 22 U.S.C. § 5511 (Supp. II 1990) (directing the Secretary of State to establish a BBS to make information contained in the Bureau of Diplomatic Security's Overseas Security BBS available to the public); 35 U.S.C. § 41(i)(2) (Supp. IV 1992) (requiring the Patent and Trademark Office to use a BBS to allow for public searches); O'Harrow, supra note 17, at B1 (noting that federal BBS topics include entry-level jobs and space shuttle flights); U.S. Agency Made Computer Virus Programs Available to Public, SAN JOSE MERCURY NEWS, June 19, 1993, at 10D (describing how a Treasury Department BBS made the source code for viruses and hackers tools available to the public). To facilitate access to the various federal BBSs, a unit of the Commerce Department sponsors the FedWorld Gateway, a gateway to over 100 different federal BBSs. Browning, supra note 20, at 1629.

RECOGNIZING LEGAL DIFFERENCES IN BBSs

and municipal levels, such as Santa Monica’s Public Electronic Network (PEN). Some universities use BBSs as well.

Wide area networks (WANs), the final segment of the BBS industry discussed here, are not technically BBS technology but are so integral to the functioning of BBSs that they deserve mention. WANs electronically connect stand-alone computer systems and networks nationally and internationally. The most prominent WAN is Internet, which has evolved from networks established by the Department of Defense and the National Science Foundation. Internet connects various government, university, and corporate entities, spans 137 nations, and has at least fifteen million users. Through the USENET BBS, carried over Internet, and other online resources, Internet users can perform all the functions available to BBS users.

Other WANs include BITNET, a network sponsored by the City University of New York, and FidoNet, a “virtual network” of 10,000 BBSs that automatically exchange private e-mail and public messages.

75. Pitta, supra note 18, at 132. This public electronic network has 300 topics, not limited to political discussions, and residents without computers can access a public computer terminal at the county library. Id. PEN is an active BBS that receives approximately 7000 calls per month. Pancho Doll, A Quiet Revolution: Computer Bulletin Boards Have Captivated the Attention of County Users, L.A. TIMES, Sept. 30, 1993, Ventura West edition, at J6 (comparing response to Ojai’s community BBS, which received only 288 calls in its first year). In Fairfax County, Virginia, elementary school principals communicate using a BBS. O’Harrow, supra note 17, at B1. See generally Tom Abate, Bay Area Cities Going On-Line; Computers, Cable TV and High-Tech Phone Systems Keep Government Open 24 Hours a Day, S.F. EXAMINER, Nov. 7, 1993, at B1 (describing the numerous efforts by Bay Area cities to establish BBSs or on-line access).

76. For example, the University of Tennessee, Knoxville, supports the Health & Safety Systems BBS, which distributes health information. Becker, Bulletin Board Operators, supra note 5, at 208 n.23.

77. One of the advantages of a network like the Internet is that users can communicate nationwide and internationally without incurring long distance telephone charges. Berck, supra note 10, at 12.

78. Internet connects over 12,000 stand-alone computer networks. Lazzareschi, Wired, supra note 69, at D2.


81. John Markoff, Thing: The Internet, N.Y. TIMES, Sept. 5, 1993, § 9, at 11; see Jim Warren, The Online Presidential Debate, MICROTIMES, July 20, 1992, at 30 (estimating that the USENET BBS, carried over the Internet, has one to three million users).

82. See Tenopir, supra note 79, at 102, 104.


84. See id. at 367-68, 370-71 (explaining that FidoNet has 500,000 users worldwide and carries three megabytes of information a day); see also Balas, supra note 9, at 26 (describing the history of FidoNet and Echomail); Alex Barnum, The Boom in Bulletin Boards:
WANs will become increasingly important given the passage in 1991 of Vice President (then Senator) Gore's National Research and Education Network (NREN) legislation. NREN will create a national information infrastructure, or electronic superhighway, for high-volume information transmission. This infrastructure may provide linkages between all BBSs and electronic networks nationwide. It may also support the development of entrepreneurial for-profit network nodes, where BBSs or other information providers can cost-effectively access the national market. This could lead to a major increase in entrepreneurial activity in the BBS industry.

B. The Sysop's Control

As part of the process of establishing and maintaining a BBS, a sysop must make business judgments in a number of areas. These areas range from financial and mechanical, such as the types of hardware and software used, to operational, such as access and monitoring policies, to the BBS's culture and "space." Although certain sysop profiles recur, it is impossible to describe a meaningful or legally useful "typical" sysop, because each sysop makes a different combination of choices.


86. See generally BECKER, PC COMMUNICATIONS, supra note 3, at 341-60; ROSE & WALLACE, supra note 1, at 17-23.

87. See generally BECKER, PC COMMUNICATIONS, supra note 3, at 333.

88. David R. Johnson & Kevin A. Marks, Mapping Electronic Data Communications onto Existing Legal Metaphors: Should We Let Our Conscience (and Our Contracts) Be Our Guide? 38 VILL. L. REV. 487, 511-12 (1993) ("[A] sysop can, in general, first decide how he or she wants the electronic 'space' to be configured. . . .")

89. One commentator suggested that all sysops have the following characteristics: (1) they invest time and money to establish the BBS, (2) they set up the BBS but otherwise do not participate in the information exchange between members, and (3) they do not know who the members are. See Beall, supra note 13, at 512; see also McDaniel, supra note 7 (developing rules to apply generically to all BBSs).

These stereotypes are not necessarily accurate. Some sysops set up their BBS so that they can interact with other users, see supra notes 66-67, and systems like Prodigy interact with every user on every message through their screening mechanism. See supra note 54. Also, most BBSs no longer accept anonymous users. See supra note 16. Therefore, the variability of sysop behavior poses some problems when rigid rules are intended to apply to all sysops.

C. BBS Functions

Many different functions are available to BBS users. As this Essay will later develop, \(^9\) these functions prove critical in determining sysops' and users' legal rights and obligations.

1. Message Functions

One of the most popular BBS functions is the ability to post public messages instantaneously. Users can opine, share information, or engage in spirited discussions with other users on a dazzling diversity of topics. \(^2\) After reviewing a list of discussion topics, the user can post a message under either a general topic, accessible by the entire BBS user base, or under one of the special interest topics. The posted messages then become part of an archive, and subsequent users may browse old messages and trace the "threads" of various debates and lines of conversation.

In addition to public message posting, users may send private electronic messages to other users directly, either internally to users of other BBSs or to global networks. For example, CompuServe’s e-mail system can communicate externally with systems such as Internet, MCI Mail, Telex, and AT&T Mail, and can fax documents to any fax machine. \(^3\) Although e-mail is generally private, the difference in audience between publicly-posted messages and private e-mail can be slight when users send e-mails to mass electronic mailing lists \(^4\) or list servers. \(^5\)

\(^{91}\) See infra part IV.B.


\(^{93}\) CompuServe Brochure, supra note 92. Most national BBSs now support some level of Internet access. Oakes, supra note 70, at 30.

\(^{94}\) For example, in response to what was considered onerous screening in Prodigy discussion forums, users created mailing lists that had up to 1500 readers and were distributed regularly. Gaffin, supra note 54.

\(^{95}\) Unmoderated list servers automatically forward messages sent to the server to a mailing list created either by an individual or subscribed to by interested parties. In many ways, the mechanics of an unmoderated list server resemble gateways. See infra part II.C.3.
Although the public and private message functions described above are asynchronous, many BBSs also allow users to communicate with each other in "real time." Real-time conferences can range from informal user-to-user "chatter" to committee meetings or press conferences. Although one of the attractions of real-time conferencing is spontaneity, some sysops exercise control over these conferences. However, users may exercise control themselves by taking a real-time discussion into a private "room." On many BBSs, users may also interact with each other in real-time through on-line games.

2. User/System Interaction and Information Services

The messaging functions listed above involve users communicating with other users, but BBSs also allow users to interact with the computer system. Such interaction may be one of five types: advertising, shopping, information databases, information storage, and software distribution.

96. The differences between public message posting, electronic mail, and real-time conferencing may blur as the technology evolves. Becker, PC Communications, supra note 3, at 185.

97. For example, CompuServe’s CB Simulator has a communication dynamic similar to that on citizens’ band radios. See Becker, Bulletin Board Operators, supra note 5, at 212. Another analogy is “900” telephone party lines, where people call in and converse while everyone else listens.

The different applications of real-time conferencing can be seen by comparing the formality of GEnie’s Real-Time Conferencing system, where users can send scrambled messages, kill the statements of troublesome users, identify the real names of users, and see who is in other private conferences, with GEnie’s more casual LiveWire Chatlines, where users adopt a “handle” (pseudonym) to conceal their true identities and choose from 40 different channels. See Becker, PC Communications, supra note 3, at 310-11.

98. Becker, Bulletin Board Operators, supra note 5, at 212. MENSA, the national high IQ society, has on-line meetings on CompuServe. CompuServe Brochure, supra note 92.

99. See Becker, PC Communications, supra note 3, at 308-09 (explaining that GEnie’s real-time conferences have leaders who can deny access to users, eject users from the conference, and require speakers to be recognized before they are allowed to post messages).

100. Becker, Bulletin Board Operators, supra note 5, at 212 n.38.

101. See Becker, PC Communications, supra note 3, at 143. On Prodigy, interactive games include GUTS, a nationwide trivia contest, and CEO, a simulation where players manage their own companies in an interactive economy. Prodigy Brochure (1992); see Potts, supra note 57, at F1 (describing how CompuServe, Prodigy, and America Online offer interactive baseball fantasy leagues and role-playing games).

The Internet also supports real-time communications and games. Some of the more bizarre offerings of the Internet are multi-user dungeons (MUDs), which attempt to create real-time virtual reality where users assume personas and explore "rooms" through a progressive series of questions and answers. See Ellen Germain, In the Jungle of MUD, Time, Sept. 13, 1993, at 61; Oakes, supra note 70, at 33.
The first type of user/system interaction is advertising. BBS technology supports both direct company advertising and product announcements. Virtually every Prodigy computer screen has an advertisement, and some companies use their own BBSs to advertise their products.

Shopping is a second category of user/system interaction. Most national commercial BBSs have "shopping malls" or electronic catalogues that allow users to buy a range of products and services. For example, CompuServe has an electronic shopping mall with 100 retailers, on-line airline, car, and hotel reservations, and on-line stockbrokers who can execute buy or sell orders.

Information databases are a third type of user/system interaction. CompuServe provides access to investment services, the full text of 700 publications, MEDLINE, a database of movie reviews, Census Bureau demographic data, national white page and yellow page telephone number directories, and Department of State travel advisories. In addition, some BBSs develop databases exclusively for their users.

A partial survey of the resources available on Internet demonstrates the power of BBSs to distribute information. Accessible databases include reference works such as the Concise Oxford English

102. Advertising occupies approximately one quarter of each screen. Reidy, supra note 34, at 35. The advertising is interspersed with substantive text, much like print media mixes text and advertising on the same page or television commercials interrupt a television show. When users ask for more information about an advertised product, the advertiser pays a fee to Prodigy. Markoff, Home-Computer Network, supra note 33, at D5.

103. See Barnum, supra note 84, at 1F (describing a BBS set up by a software vendor for customer service that advertises the company's products).

104. When acting as a conduit between the user and the retailer, the BBS functions as a gateway. See infra part II.C.3.

105. Flynn, supra note 56, at 1F. CompuServe also has a "new car showroom," a classified ads section, and a discount shopping club called "Shoppers Advantage." CompuServe Brochure, supra note 92.

106. CompuServe Brochure, supra note 92.

107. These include Disclosure (financial statements), FundWatch Online, Standard & Poor's, and Value Line. Id.


110. CompuServe Brochure, supra note 92.

111. Id.

112. These databases can include lists of other BBSs that act as gateways for certain networks, lists of viruses, and BBS membership lists. Rose & Wallace, supra note 1, at 57.
Dictionary, Oxford Thesaurus, and Peterson’s College Directory, electronic journals and newsletters, and computer-encoded books such as Moby Dick, The Federalist Papers, The Book of Mormon, and the complete works of Shakespeare.\(^{113}\)

Data storage is a fourth type of user/system interaction. Most BBSs allow users to store information and data on the system computer. This information can be either electronically transmitted to the user from an external source, downloaded (received)\(^{114}\) from the BBS’s databases, or uploaded (sent)\(^{115}\) by the user to the BBS computer’s hard drive.

Software exchange is the fifth and final category of user/system interaction. Most BBSs allow users to upload and download software.\(^{116}\) Because of this, BBSs have become major software distributors.\(^{117}\) BBSs often build their reputations on the quality and quantity of their downloadable software.\(^{118}\) While much of the software available is “public domain,” “freeware,” or “shareware,”\(^{119}\) copyrighted software that has been illegally copied can be found on some BBSs.\(^{120}\) Other problems with the distribution of software by

---

\(^{113}\) Tenopir, *supra* note 79, at 102, 104.

\(^{114}\) “Downloading” occurs when the user copies information or software from the BBS onto the user’s computer.

\(^{115}\) “Uploading” occurs when the user copies information or software from the user’s computer to the BBS.


\(^{117}\) “Because shareware depends largely on [BBSs] for its distribution and advertising, the continued growth of the BBS community will provide a stronger and more widespread network for the distribution of archived shareware. Many bulletin boards boast shareware libraries that fill several hundred megabytes of hard disk space.” Becker, *PC Communications, supra* note 3, at 104.

\(^{118}\) BBS etiquette dictates that users who download software should upload software in return. See id. at 334; cf. Becker, *Bulletin Board Operators, supra* note 5, at 210 n.28 (describing how one “pirate” BBS conditioned access to software on the user having contributed pirated software). See generally Rose & Wallace, *supra* note 1, at 29 (discussing how some sysops impose upload/download ratio requirements).

\(^{119}\) “Public domain software” is software that the programmer does not copyright and dedicates to the public domain. “Freeware” is software that the programmer copyrights but makes available for free. “Shareware” is copyrighted software that the programmer makes available without charge; those users who keep and use the software are obligated, however, to pay the programmer for the software. See Becker, *PC Communications, supra* note 3, at 81-84.

\(^{120}\) See, e.g., Joe Abernathy, *Federal Agents Raid Dorms, Seize Computer Equipment*, Hous. Chron., Dec. 17, 1992, at A1 (“There are a lot of underground sites on the Internet . . . . [that] have tons of software available to download—gigabytes of software . . . . . . There’s no way that one agency or authority can go through and try to sweep all the bad software
BBSs include the spread of computer viruses and the presence of files which users may find indecent, pornographic, or obscene.

3. "Gateways"

One of the unique features of a BBS, compared with other technologies, is the ability to act as a gateway. A gateway allows the computer to communicate electronically with other computers, so that the BBS user can perform activities on the external computer system. Information passing through the gateway computer is briefly processed by the gateway's computer hardware before being sent to the intermediate or destination computer for further processing. When CompuServe users access another company's proprietary database (such as Dow Jones), CompuServe is acting as a gateway between the user and the Dow Jones database. Similarly, when CompuServe users access the Internet, CompuServe is a gateway to the Internet gateway, which connects the user's computer to a destination network system.

III
Analysis of the Implications of Various Legal Analogies as Applied to the BBS Context

A. Synopses of the Rights and Obligations Involved with Each Analogy

Having offered some background into the functional and industry context of BBSs in the previous part, this Essay will now outline the law that applies in analogous situations. The Essay focuses on three categories: (1) the extent of the government regulatory scheme; (2) off the Internet, because the Internet's too big.

121. Viruses cause the user's computer to do something unexpected and unwanted, ranging from the innocuous (e.g., displaying the name of the virus's author) to the catastrophic (e.g., erasing the entire contents of a user's hard disk). See Becker, PC Communications, supra note 3, at 107-09. See generally Rose & Wallace, supra note 1, at 155-57 (distinguishing between viruses, trojans, worms, and time bombs).

Because BBSs historically have been a major transmitter of viruses, many BBSs automatically scan uploaded software to detect viruses. Becker, PC Communications, supra note 3, at 112.

122. See Becker, PC Communications, supra note 3, at 169, 368.

123. Id. at 362.

124. The Internet acts as a gateway in connecting e-mail users on different systems, but it can also provide a gateway to commercial information databases such as Dialog. Tenopir, supra note 79, at 102, 104.

125. Commentators have also analogized BBSs to:

the owner's right of control and the user's right to access; and (3) the
owner's liability for the statements of others. This subpart will pro-
vide a common framework of the general rules, but will not explore
the nuances of various legal models. Once the framework is estab-
lished, the next subpart will evaluate each analogy's strengths and
weaknesses from a policy perspective, as applied to both users and
sysops.126

The types of entities considered as analogous to BBSs include
print publishers (primary publishers and republishers), secondary
publishers (including booksellers, news distributors, libraries, and, for
defamation liability purposes, telegraph companies),127 broadcasters,
common carriers, and private real and personal property owners.128

At the end of this subpart, an analysis of the public forum doctrine
outlines some rules that apply to state actors.

1. The Extent of Government Regulation

Some media, such as broadcasters and common carriers, are sub-
ject to extensive government regulation. For example, because of per-
ceived spectrum scarcity, the FCC allocates the broadcast spectrum to

126. This is important to protect both the sysops' freedom and the users' right to free
speech, although these rights necessarily conflict. Cf. Henry H. Perritt, Jr., Tort Liability,
the First Amendment, and Equal Access to Electronic Networks, 5 HARV. J.L. & TECH. 65,
71 (1992) [hereinafter Perritt, Tort Liability] (enumerating such goals as diversity of opin-
ions, low access barriers, and victim compensation). Currently, the law favors owners' First
Amendment rights and there is a danger that focusing on sysop liability will reinforce this
existing favoritism to the detriment of the First Amendment rights of listeners or users.
See POOL, supra note 18, at 133; ROSE & WALLACE, supra note 1, at 19.

127. For the purposes of defamation, telegraph companies are included as secondary
publishers. See W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS
§ 113, at 811-12 (5th ed. 1984); RESTATEMENT (SECOND) OF TORTS § 581(1), cmt. f (1976);
see also Becker, Bulletin Board Operators, supra note 5, at 214.

128. Other analogies also could be considered, such as enhanced service providers (as
defined by the FCC) and cablecasters, but for the relevant analysis these other situations
merge with one of the five types discussed.
ensure that it is being used to benefit the public.129 The FCC only grants licenses for a limited time period130 and may restrict ownership.131 In response to the potential for monopolistic situations, Congress has similarly enacted a broad scheme of telephone and telegraph regulations.132

In contrast, government intrusion into print publishing is severely restricted both constitutionally and statutorily. For instance, the U.S. Supreme Court held that a use tax on ink and paper, with its detrimental impact on print publishers, was an unconstitutional infringement of print publishers’ freedom.133 Before searching or seizing print publishers’ work product or documentary materials, the government must make a heightened showing of need.134 Congress, recognizing the important role of newspapers, has exempted newspapers from some antitrust prohibitions.135

Similarly, whether based on the owner’s First Amendment protections or the Fifth Amendment Takings Clause, the government is also prohibited from dictating the use of private property for communications purposes.136

2. Owner’s Extent of Control/User’s Right to Access

In general, there is a sliding scale of control in relation to forced access. At one end of the scale are primary publishers, who have virtually unrestrained discretion over what they print or to whom they give access to disseminate information.137 Also on this end are owners of private property, who are similarly protected from mandatory or

129. See Tribe, American Constitutional Law, supra note 41, at 1004.
130. 47 U.S.C. § 307(c) (1988). The power to license can take the form of content regulation. See Pool, supra note 18, at 134-35; infra notes 148, 222 and accompanying text.
131. 47 U.S.C. § 310 (1988) (restricting foreigners from obtaining broadcasting licenses); id. § 533(a) (restricting single entities from owning television stations and cable television systems in the same market).
132. Id. §§ 201-224. Pool also notes that Congress allows taxes on phone bills but the Supreme Court prohibited an identical tax on newspapers in Minneapolis Star & Tribune Co. v. Minnesota Commissioner of Revenue, 460 U.S. 575 (1983). Pool, supra note 18, at 106.
136. See Wooley v. Maynard, 430 U.S. 705, 715 (1977) (striking down New Hampshire’s “Live Free or Die” license plate because the state had compelled its citizens to “use their private property as a ‘mobile billboard’ for the State’s ideological message”).
forced access. In some cases, government-mandated access could be considered a taking. However, the rights of private property owners have been restricted in one key respect. As an extension of the public forum doctrine, if private property resembles a traditional government-owned or -controlled public forum, the Court has been willing to consider permitting government-mandated access. Thus, although speakers do not have a right of access to private property under the U.S. Constitution, the Court has held that states may, on independent state grounds, require private owners to permit individuals to exercise free speech on private property in limited circumstances.

Further along the sliding scale of control and forced access lies broadcasting, about which Laurence Tribe has noted, "[f]rom the beginning, the federal government—by its licensing practices and by rules directed at the substantive content of broadcasting—has strongly influenced what broadcasters have had to say." For example, under the Equal Opportunities Doctrine, broadcasters who provide access to one political candidate must offer equal opportunity to competing candidates and may not censor these broadcasts. Broadcasters have

---


139. See Loretto v. Teleprompter Manhattan CATV Corp., 458 U.S. 419 (1982) (holding that a New York law requiring apartment buildings to give access to cable companies constituted a taking). However, the Court may be more deferential to government-imposed burdens in cyberspace (as opposed to takings in physical space). Cf. Tribe, American Constitutional Law, supra note 41, at 1008 (noting that the Equal Opportunities Doctrine, which requires broadcasters to allow political candidates to use the broadcasting facilities, apparently does not raise a takings issue).


141. Hudgens v. NLRB, 424 U.S. 507 (1976). In Hudgens, the Court rejected a First Amendment challenge to a private shopping center owner's restrictions on a labor union that wanted to picket a store in the center. Tribe argues that the Hudgens court was sympathetic to the First Amendment interests of shopping center owners not to use their property to support someone else's ideology. See Tribe, American Constitutional Law, supra note 41, at 1000.

142. PruneYard, 447 U.S. 74. The Court gave three reasons: (1) the states' inability to mandate access could greatly restrain speakers' ability to communicate their messages; (2) if the mandated access was content-neutral, there would be no discrimination problem; and (3) shopping centers are generally considered inherently public, so audiences will not perceive the owner as the speaker. Id. at 87. See generally Di Lello, supra note 28, at 225-26 (outlining which states' laws favor property owners and which states' laws favor speakers).

143. Tribe, American Constitutional Law, supra note 41, at 1002 n.35. Tribe continued: "The first amendment's sweeping guarantees have been most compromised in the realm of ... electronic broadcasting." Id. at 1004.

144. 47 U.S.C. § 315(a) (1988). The Equal Opportunities Doctrine also restricts the amount that can be charged to these candidates for their use of broadcast stations. Id. § 315(b).
discretion to reject editorial advertising, but the FCC may revoke a station's license if it does not provide "reasonable access" to candidates for federal office. Additionally, broadcasters have no discretion to accept cigarette advertising. Finally, the FCC may control content, such as the publication of indecent words.

At the other end of the sliding scale from primary publishers are common carriers, who by definition must be available to all comers and cannot refuse to provide service in a discriminatory fashion. This open access generally means that the carrier cannot distinguish between customers based on content, and government control over the right of access is restricted. Therefore, in Sable Communication v. FCC, the U.S. Supreme Court found that the FCC's ban of "indecent" telephone communications was unconstitutional, since it exceeded what was necessary to serve the compelling government interests involved.

In some respects, secondary publishers are similar to common carriers, because secondary publishers also do not exercise editorial control over content. However, this analogy is not complete, because secondary publishers do not necessarily have to allow unrestricted access. For example, in Board of Education v. Pico, the Court permit-
ted school libraries to exercise some discretion over which books are placed on their shelves, but once a book is placed on its shelves, the library may not remove the book merely because the library disagrees with the book's contents. While *Pico* was limited to state actors, a broad reading of the rule could apply to private secondary publishers, who would be permitted to choose who gets access but, once an entity is given access, could not censor content for arbitrary reasons. However, in the absence of such a broad reading of *Pico*, there is no general right of access to private secondary publishers.

3. Owner's Liability for the Statements or Actions of Others

The sliding scale of control and access described in the previous subpart also applies here: Those entities with more editorial control generally also have greater exposure to tort liability for the statements or actions of others. Therefore, primary publishers, who have the greatest control, also have the greatest exposure to defamation liability. Primary publishers may be liable for defamation in the case of public officials and other public figures only if they have actual malice (including recklessness); otherwise, states may hold primary publishers liable under a negligence standard. In *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, the Court held that a private commercial information distributor could be held liable for presumed damages without a showing of "actual malice" if the issue was not a public concern. Although the strict standards of defamation liability have historically applied only to news media entities, language in *Dun & Bradstreet* indicates that the rules will be applied consistently to both media and nonmedia primary publishers.

In addition to defamation liability, primary publishers may be liable for other types of statements. For example, a print publisher may be liable for compensatory damages for publishing commercial adver-

---

154. *Id.* at 870-72 (Brennan, J., plurality opinion).
158. *Id.* at 761 (Powell, J., plurality opinion). The private/public distinction is less tenuous now that the type of credit information at issue in *Greenmoss Builders* is routinely made available on-line to thousands of subscribers. *Tribe, American Constitutional Law*, supra note 41, at 1009 n.76.
159. 472 U.S. at 773 (White, J., concurring in the judgment); *accord id.* at 782 n.7 (Brennan, J., dissenting) ("[T]here has been an increasing convergence of what might be labeled 'media' and 'nonmedia.'")
tisements that pose a substantial danger of causing harm if the danger is apparent on the advertisement's face.\textsuperscript{160}

However, where primary publishers exercise only limited editorial control, traditional standards may not apply. In other words, when primary publishers act as a conduit for other people's statements, such as when they report defamatory statements as news, primary publishers may benefit from a more lenient standard. For example, in \textit{Edwards v. National Audubon Society, Inc.},\textsuperscript{161} the Second Circuit Court of Appeals held that \textit{The New York Times} was not liable for defamation when it merely reported defamatory allegations made by the "responsible [and] prominent" National Audubon Society, even if the publisher did not independently investigate the allegations.\textsuperscript{162}

Most broadcasters exercise editorial control as vigorously as do primary publishers. As a result, broadcasters' liability for defamation does not differ from print publishers' liability,\textsuperscript{163} and the scienter requirements are the same.\textsuperscript{164} However, in contexts where broadcasters have only limited control, their liability also appears to scale back proportionately. Therefore, in \textit{Farmers Education and Cooperative Union v. WDAY, Inc.},\textsuperscript{165} the Court held that, because the Equal Opportunities Doctrine\textsuperscript{166} required the defendant radio station effectively to turn control of the broadcast content over to the candidate making defamatory statements, the station was not liable for these statements.\textsuperscript{167}

Continuing on the sliding scale, private property owners who have extensive control over the use of their property for communication purposes can be liable for defamation if they meet the require-

\begin{itemize}
  \item \textsuperscript{161} 556 F.2d 113 (2d Cir.), cert. denied, 434 U.S. 1002 (1977).
  \item \textsuperscript{162} \textit{Id.} at 120. In \textit{Edwards}, \textit{the New York Times} was sued after it reported allegedly defamatory statements. The National Audubon Society had challenged statistics regarding the effects of the pesticide DDT on the bird population and said that any scientist who used the evidence to support the continued use of DDT "is being paid to lie, or is parroting something he knows little about." \textit{Id.} at 118.
  \item \textsuperscript{163} Becker, \textit{Electronic Publishing, supra} note 24, at 849.
  \item \textsuperscript{164} \textit{Restatement (Second) of Torts} § 581 (1977); \textit{accord Keeton et al., supra} note 127, at 812.
  \item \textsuperscript{165} 360 U.S. 525 (1959). The Court's holding apparently applies even if the broadcaster could have used an electronic delay system. \textit{Keeton et al., supra} note 127, at 812.
  \item \textsuperscript{166} The Equal Opportunities Doctrine at issue in \textit{WDAY} was similar to 47 U.S.C. § 315(a).
  \item \textsuperscript{167} 360 U.S. at 531.
\end{itemize}
ments for becoming a republisher. Therefore, private property owners can be liable for the defamatory statements of others if they control land or chattels and intentionally and unreasonably fail to remove defamatory matter that they know is exhibited.168

With no real editorial control, secondary publishers are liable for defamatory statements by others only if they "knew or had reason to know of the existence of defamatory material contained in the matter published . . . [unless] (a) the originator had a privilege or (b) the disseminator reasonably believed that the originator had a privilege."169 This general immunity from liability for others' statements applies in other contexts, such as the transmission of obscenity. In Smith v. California,170 the Court struck down a Los Angeles municipal ordinance that held booksellers strictly liable for possessing obscene material, reasoning that requiring booksellers to review all the books they sold would decrease public access to books, including books containing constitutionally protected expression.171 This illustrates that the basis for finding an absence of liability for other people's statements is partly a concern that imposing liability would lead to greater control which, in turn, would inhibit constitutionally protected speech.

---

168. Reprintation (Second) of Torts § 577(2) (1976); see, e.g., Hellar v. Bianco, 244 P.2d 757 (Cal. Ct. App. 1952). In Hellar, the defamatory statement involved was "ask for Isabelle" and a phone number, written on the bathroom wall of a bar. After a patron called the woman in question, the woman's husband demanded that the statement be removed, which the bartender failed to do "after some delay." Id. at 758-59. The court held that, in places of public accommodation, the landlord must remove publicly visible defamatory statements within a reasonable time or the landlord may be held liable for republication. Id.; see Restatement (Second) of Torts § 577(2), cmt. p & illus. 15 (1976) (noting, however, that landlords do not have a duty to police the property or chattel). But see Scott v. Hull, 259 N.E.2d 160 (Ohio Ct. App. 1970) (explaining that even if owner has notice, owner is not liable for visible defamatory graffiti, since nonfeasance does not create defamation liability).

Numerous commentators have tried to reconcile the conflicting Hellar and Hull approaches. See, e.g., John R. Kahn, Defamation Liability of Computerized Bulletin Board Operators and Problems of Proof, Feb. 1989, available in Internet via gopher, gopher.eff.org; Loundy, supra note 45, at 146-48.

169. Keeton et al., supra note 127, at 811; see Restatement (Second) of Torts § 612 (1976).


171. Id. at 153-54. However, by expressly limiting its holding to strict liability in a criminal context, the Court did not preclude criminal liability based on scienter. Id. at 154. Further, Smith would not apply to a question of civil liability based on scienter. See, e.g., Perritt, Tort Liability, supra note 126, at 105 (giving a hypothetical situation in which a bookseller knew a book contained defamatory statements, and presuming such knowledge would make the bookseller liable as a republisher).
Finally, common carriers, such as telephone companies, mail carriers, and other non-content providers like equipment providers, also lack substantial editorial control and generally are considered immune from liability for the statements of others in the absence of some aggravating circumstance. Therefore, in Anderson v. New York Telephone Co., the telephone company was not liable for a user's defamatory answering machine message even when the telephone company knew about the defamatory statements. Without this type of immunity, common carriers would be forced to prescreen, which would cause them to operate less efficiently and would be contrary to the users' expectations of privacy.

B. State Actors and the Public Forum Doctrine

The public forum doctrine applies only to "state owned, operated, or sponsored computer systems." If the BBS is a state actor, the BBS's ability to act will be determined by the type of forum it is

172. See Perritt, Tort Liability, supra note 126, at 103 n.195; McDaniel, supra note 7, at 824 (treating "contract printers" as secondary publishers).
173. See Restatement (Second) of Torts § 612(2) (1976); see also Charles, supra note 125, at 132 n.72 (listing cases that hold a common carrier is not liable for defamation).
175. Charles, supra note 125, at 143.
176. A forum has the following elements: "(1) a location, (2) accessible to, (3) segments of the population, (4) where the discussion of issues occurs." Taviss, supra note 39, at 760. Although BBSs lack a physical location, id., so do public forums such as government publications and mail systems. Therefore, a BBS can and should be considered a forum located in cyberspace. See supra note 1.
177. Taviss, supra note 39, at 781-82. For purposes of public forum analysis, private actors are state actors if either the private actor performs a public function or the state is entangled with private actors. Id. at 767-68 & n.69. Taviss concludes that privately-owned BBSs do not perform a public function because the state does not traditionally own BBSs, id. at 770, and they will not be entangled unless the state is extensively involved in operating the BBS or affirmatively exercises licensing power. Id. at 772-73. Even if gateways such as Internet are state actors, this is not sufficient to entangle all communication transmitted by the gateway. Id. at 784-85. Taviss concludes that the increasing importance and ubiquity of computer-based communication could eventually lead to enough entanglement to make all BBSs state actors. Id. at 791; accord Pool, supra note 18, at 41; Oldenburg, The Law, supra note 45, at E5 (quoting Laurence Tribe). Alternatively, Congress could convert private BBSs into state actors using the Commerce Clause. Taviss, supra note 39, at 792 & n.264; cf. Di Lello, supra note 28, at 241 (arguing for Congress to enact legislation, using the Commerce Clause, to prohibit commercial BBSs from censoring or ejecting users). But cf. Pool, supra note 18, at 91-92 (early regulation of telegraphy under the Commerce Clause probably should have been subordinated to First Amendment interests).
deemed to be. The three type of forums described by the U.S. Supreme Court are:178

(1) The “traditional public forum.” Based primarily on historical usage, traditional public forums are narrowly defined as parks, public streets and sidewalks,179 not BBSs.180 In traditional public forums, the Court applies strict scrutiny181 to content-based restrictions on speech and intermediate scrutiny182 to content-neutral time, place, and manner restrictions.183

(2) The “limited public forum.” Limited public forums exist when the state actor intentionally creates a forum and makes it available to the public.184 The Court applies strict scrutiny to content-based restrictions in limited public forums.185 Time, place, and manner restrictions in such forums must be reasonable.186 State-owned BBSs set up for the purpose of facilitating interactive communication with the government and other citizens could be considered limited public forums, subject to the state actor’s right to shut down the forum and to impose time, place, and manner restrictions.187

179. Perry, 460 U.S. at 45.
180. In some respects, BBS technology demonstrates that strict adherence to physical-based definitions turns constitutional protections on their head. See supra text accompanying notes 35-38. Because BBSs are extremely powerful vehicles for political expression and protest, see supra text accompanying notes 19-23, liberal access to “traditional” public forums without concomitant liberal access to electronic media may in time undermine the free marketplace of ideas. Cf. Naughton, supra note 19, at 431 (“For a substantial population, the electronic arenas of computer networks have displaced the nation’s streets and parks as the quintessential public fora. . . . [C]omputer networks enable users to disseminate their ideas to a far broader audience than any traditional public forum.”). Ultimately, if BBSs become a predominant communication medium, see supra note 39, courts should reexamine the policy considerations underlying the limiting of special legal solicitude to “traditional” public forums.
181. In order for a regulation to be upheld under strict scrutiny, the regulation must be “necessary to serve a compelling state interest and . . . narrowly drawn to achieve that end.” Perry, 460 U.S. at 45.
182. In order for a regulation to meet the intermediate scrutiny standard, it must be “narrowly tailored to serve a significant government interest, and leave open ample alternative channels of communication.” Id.
183. Id.
184. Cornelius v. NAACP Legal Defense & Educ. Fund, Inc., 473 U.S. 788, 802 (1985). Taviss argues that, especially given the courts’ deference to free speech on campuses, courts should treat university-based BBSs and computer systems as limited public forums, Taviss, supra note 39, at 789-90, or legislation should be passed to declare academic-based BBSs and computer systems to be limited public forums. Id. at 791-92.
185. Perry, 460 U.S. at 45-46.
186. Id.
187. Taviss, supra note 39, at 787-88. These interactive BBSs include Santa Monica’s PEN, id. at 788, and BBSs (such as Montana’s) that are designed to promote constituent/
RECOGNIZING LEGAL DIFFERENCES IN BBSs

(3) The "nonpublic forum." A nonpublic forum is defined as "[p]ublic property which is not by tradition or designation a forum for public communication." State actors can restrict access and impose reasonable regulations, including those which discriminate on the basis of content.

C. Policy Considerations—The Merits of BBSs and Interest Balancing

Given the range of legal rights and obligations outlined in subparts A and B above, an important issue is determining which distinguishing characteristics of BBSs warrant special consideration in selecting the appropriate levels of legal rights and obligations. One commentator has posited BBSs are unique because of the speed and low cost of BBS-based communication. Certainly speed is no small factor. The fact that speakers may disseminate their ideas on demand, and in some cases interact with each other contemporaneously, compares favorably with "slow" technologies such as publishing and broadcasting. The fast speed also allows faulty or imprecise information to be corrected rapidly, creating a dynamic information marketplace.

The low cost of BBSs is another important factor, particularly regarding free BBSs that are essentially electronic "traditional public forums." Indeed, as the poor person's mass media vehicle, BBSs can be the only cost-effective and meaningful way for some individuals to command the attention of an audience. The low cost can also help create "inverted pyramids," where individuals who have low sta-

---

188. Perry, 460 U.S. at 46.

189. Id.

190. Charles, supra note 125, at 143.


192. See Naughton, supra note 19, at 429 ("A computer network has many of the attributes of a traditional public forum.").

193. For example, BBS's speed and low access costs allow defamed individuals to respond immediately on the same BBS and with the same intensity, undermining some of the underpinnings of defamation jurisprudence. Edward A. Cavazos, Note, Computer Bulletin Board Systems and the Right of Reply: Redefining Defamation Liability for a New Technology, 12 REV. LITIG. 231, 246-47 (1992); see Cutrera, Computer Networks, supra note 16, at 570.
tus in the physical world can gain prominence and notoriety in the online world.\textsuperscript{194}

In addition to beneficial effects on communication, the speed and cost-effectiveness of BBSs can lead to the instantaneous and low-cost formation of interest-based groups, without regard to any user's geography or demographic characteristics.\textsuperscript{195} BBS users can cost-effectively find others with whom to affiliate and can engage in wide-ranging, socially-enriching dialogue,\textsuperscript{196} in effect creating a decentralized information economy.\textsuperscript{197} These decentralized and geographically disparate groups frequently develop altruistic community norms, which are even found in situations in which the cost for individuals to assist other users exceeds their personal benefits.\textsuperscript{198} The combination of a global scope of communication, altruism contrary to economic theory, and immediate on-line intimacy makes the BBS an empowering tool.\textsuperscript{199}

\textsuperscript{194} See William Grimes, Computer as a Cultural Tool: Chatter Mounts on Every Topic, N.Y. Times, Dec. 1, 1992, at C13 (citing Nancy Baym, a doctoral student in speech communications).

\textsuperscript{195} Characteristics which become irrelevant to group interaction include race, religion, sex, age, educational status, and socioeconomic status. BBSs are "a medium whose characteristics champion only 'pure' messages, stripped of physical conditions. In an electronic forum, there can be no discrimination because factors such as race, religion, and economic status, do not accompany the message." Taviss, supra note 39, at 795. As a result, "[t]here is no visual content, no hearing of accents. People are judged on the content of what they say." Bishop, supra note 125, at 3 (quoting Wayne Gregori, sysop of the SF Net). Further, because "[c]yberspace recognizes no national boundaries, and physical obstacles such as oceans and deserts that have historically compartmentalized people are non-existent... individuals are free to associate with others of their choosing...." Terri A. Cutrera, Note, The Constitution in Cyberspace: The Fundamental Rights of Computer Users, 60 UMKC L. Rev. 139, 139 (1991) [hereinafter Cutrera, The Constitution in Cyberspace].

\textsuperscript{196} "The essence of public messages and open files on a computer bulletin board is... the participation of many in the interchange of ideas, opinions, and information." Becker, Bulletin Board Operators, supra note 5, at 228; see Harmon, New Legal Frontier, supra note 26, at A24 (the low cost of group formation allows small stock market investors to pool information resources).

\textsuperscript{197} See Jon Katz, Bulletin Boards: News from Cyberspace, Rolling Stone, Apr. 15, 1993, at 35, 35 ("Armed with relatively inexpensive new technology, millions of Americans are now finding that they don't need the gatekeepers [such as the traditional media] anymore.").

\textsuperscript{198} See, e.g., Christopher J. Galvin, A World of Good, CompuServe Mag., June 1993, at 10. In his article, Galvin describes numerous examples of altruistic behavior on CompuServe. Even the merest assistance, such as answering a question posed to a conference, imposes private costs because the answerer must pay CompuServe's on-line connect charges. However, the generosity often extends to mentoring and to providing technical troubleshooting that would normally command a consulting fee. See id. at 12-13.

\textsuperscript{199} See John S. Quarterman, Network Communities Across Boundaries, Micrometimes, May 31, 1993, at 128, 128 (describing how the former Soviet Union and China, among others, appear to be restricting the development of wide area networks for fear of the subversive power of these networks); cf. Rheingold, supra note 23, at 6 ("Electronic citi-
Finally, in addition to their communication and group dynamics, BBSs are also one-stop electronic convenience stores, offering the ability to access experts or celebrities, to tap into tremendous information databases, to obtain software, to store information, and to shop. Everything that can be done in cyberspace can be done in the physical world, but the convenience and speed of BBSs can convert otherwise burdensome tasks into accessible ones.

As the above discussion indicates, BBSs have many special features that deserve protection. However, the electronic power that allows users to achieve so much that is positive also allows users to engage in social wrongs. Eventually, through either tort or criminal liability for sysops, society will decide how much BBS activity it will circumscribe both directly and indirectly.

In ascribing tort liability, it is axiomatic that the tortious user should be liable. However, if society considers sysops part of the causal link in user wrongdoing, then the tort goals of deterrence and victim compensation indicate that sysops should also be liable.


201. See supra part II.C.

202. Corporate users have found that access to information and software is both greater and quicker on the Internet. For example, one IBM researcher used the Internet to obtain technical software immediately that would have taken nine months to obtain otherwise. Eckhouse, supra note 70, at C1.

203. See Godwin, supra note 26. “People are people, even in cyberspace.” ROSE & WALLACE, supra note 1, at 67.

204. For example, in California Software, Inc. v. Reliability Research, Inc., 631 F. Supp. 1356, 1358 (C.D. Cal. 1986), the defendants sent allegedly tortious communications over a nationwide BBS. The sysops were not named as defendants. Similarly, Prodigy was not named as defendants in the Medphone case. Godwin, supra note 26.


However, victim compensation can be tricky because both the user and the sysop can be judgment-proof, and the sysop may not be able to obtain insurance. ROSE & WALLACE, supra note 1, at 88, or afford it, Jensen, supra note 18, at 247. On networks such as FidoNet, Echnonet, and USENET, victim compensation is especially problematic given that no one entity or person monitors the on-going activities of the system. See BECKER, PC COMMUNICATIONS, supra note 3, at 370, 374; ROSE & WALLACE, supra note 1, at 15; Oldenburg, The Law, supra note 45, at E5.
contrast, if society decides that BBSs have more social benefits than are reflected by BBS revenues, society should subsidize BBSs by restricting the sysop's tort liability.\textsuperscript{206}

It has been proposed that sysops should be subject to criminal liability for users' actions.\textsuperscript{207} However, criminal liability poses the dangers that sysops may inadvertently be held strictly liable for users' criminal behavior,\textsuperscript{208} or that law enforcement officials, either afraid\textsuperscript{209} or ignorant\textsuperscript{210} of computers, will use criminal liability to harass sysops and breach constitutional protections.\textsuperscript{211} While it is beyond the scope of this Essay to fully map the contours of sysops' criminal liability for the statements or actions of their users,\textsuperscript{212} a \textit{mens rea} of recklessness, at the least, should be required to impose liability, in order to avoid a chilling effect.\textsuperscript{213}

\textsuperscript{206} Jensen, \textit{ supra} note 18, at 247 n.158.


\textsuperscript{208} See \textit{id.}; cf. Uyehara, \textit{ supra} note 24, at 32 (noting that users could deliberately implicate sysops in wrongdoing by intentionally posting illegally copied software).

\textsuperscript{209} Technology phobia is not a new phenomenon. See \textit{Pool}, \textit{ supra} note 18, at 119 (noting that in the 1920s, radio "was often looked upon as a potentially . . . dangerous instrument which could, without vigilance, destroy American ideals") (footnote omitted).

\textsuperscript{210} While it is tempting to assume that law enforcement officials are technologically sophisticated, law enforcement naiveté is well documented. See \textit{Rose & Wallace, supra} note 1, at 143-45; Karlin, \textit{ supra} note 30, at T6 (quoting Jack Rickard of \textit{Boardwatch} magazine as saying that law enforcement officials are unable to distinguish between computer hobbyists and criminals); Lazzareschi, \textit{Computer Users, supra} note 40, at D9 ("[O]ne prosecuting attorney has equated a teenager with a modem to a teenager with a gun.") (quoting Mitch Kapor); Quittner, \textit{ supra} note 31, at 1 (quoting Steve Jackson, on the return of computers extensively damaged after the Secret Service had searched them for evidence: "[T]he Secret Service knows nothing about computers, and this just demonstrates it."); Uyehara, \textit{ supra} note 24, at 32 (Jeffrey Fogel, executive director of the New Jersey ACLU, responding to a prosecutor's suggestion that the legislature should license modems with "Why don't they ask legislators to license mouths?").

\textsuperscript{211} See the examples, such as the Steve Jackson and Craig Neidorf prosecutions and Operation Sun Devil, described \textit{ supra} notes 31-32. The government has admitted that Operation Sun Devil was intended to have a deterrent effect. See Cutrera, \textit{The Constitution in Cyberspace, supra} note 195, at 162. While deterring criminal activity is desirable, the Secret Service's heavy-handed tactics can also intimidate law-abiding citizens from entering the marketplace of ideas for fear of inadvertently being the Secret Service's next target.

\textsuperscript{212} Of course, sysops who use their BBSs for criminal purposes should be criminally liable. See, e.g., John Engellenner, \textit{Roseville Couple Arrested in Satellite-TV Pirating Case}, \textit{Sacramento Bee}, Dec. 11, 1992, at B1 (describing how a couple was arrested because they established and used a BBS to disseminate satellite TV descrambling codes).

\textsuperscript{213} See Jensen, \textit{ supra} note 18, at 231-32 n.79 (explaining that since sysop liability for users' actions "seems akin to that of a co-conspirator," sysop's criminal liability requires specific intent); Brock N. Meeks, \textit{As BBSes Mature, Liability Becomes an Issue}, \textit{INFOWorld}, Jan. 22, 1990, at S14, S14 (arguing that sysops should not be criminally liable for the presence of illegal material on their BBSs "unless obvious evidence exists that the sysop solicited the information").
Beyond the sysops' civil and criminal liability, there is an underlying issue of how extensively the government should intervene in the mechanical operation of private media ventures. For example, if the government does not mandate media access, then access may be restricted to powerful or wealthy individuals. Indeed, print publisher jurisprudence has acknowledged this reality. In *Miami Herald Publishing Co. v. Tornillo*, the Court noted that "economic factors . . . have made entry into the marketplace of ideas served by the print media almost impossible." However, if new BBSs may freely enter the market, power concentration or restricted access is less of a problem because users can vote with their modems or become sysops themselves. Therefore, functioning market mechanisms obviate the need for government's heavy hand.

Indeed, government intervention or excessive sysop liability may cause a chilling effect that will shrink all speech, not necessarily just speech unprotected by the Constitution. The dangerous effect of government intrusion is most obvious in the prospect of Congressional authorization of FCC control over the BBS industry. FCC regulation poses several dangers: Sysops may exit or refuse to enter the industry rather than comply with licensing obligations, private entities may be disincentivized from entering the market, and the chilling effect on speech may be more pervasive than just obscenity. Conversely, sysops who become primary publishers can be criminally liable for obscenity.

However, in a case of criminal obscenity, *Smith v. California*, 361 U.S. 147, 153-54 (1959), the Court held that secondary publishers cannot be criminally liable for distributing information. Where sysops become secondary publishers, *Smith* would dictate that these sysops are free from criminal liability for obscenity. Conversely, sysops who become primary publishers can be criminally liable for obscenity.

---

216. *Id.* at 251; cf. *Pool*, supra note 18, at 11-12 ("Publishing is rarely now the expression of just an individual. It is undertaken by large organizations.").
217. *See Henry H. Perritt, Jr., Introduction: Symposium: The Congress, The Courts and Computer Based Communications Networks: Answering Questions About Access and Content Control*, 38 VILL. L. REV. 319 (1993) [hereinafter Perritt, Symposium]; Perritt, *Tort Liability*, supra note 126, at 141; *infra* part V. However, some fear that the centralized information infrastructure, currently being built by private entities and which is expected to be the major media conduit in the future, will charge significant fees to recoup the cost of development and thereby preclude access by noncommercial disseminators. *See* Tom Abate, *What So Proudly We Logged on*, S.F. EXAMINER, July 4, 1993, at E1.
218. *See*, e.g., *Becker, Bulletin Board Operators*, supra note 5, at 230 n.125; *Beall, supra* note 13, at 511; *Gilbert, supra* note 205, at 448 n.44. As one telecommunications writer recommended, "[s]ysops can take practical steps to protect against [defamation liability] by not tolerating any types of personal attacks, even against public figures. Even if the mayor is a crook, do you [the sysop] want to spend hard-earned money proving it in court?" *Meeks, supra* note 213, at S15.
219. *See* Beall, *supra* note 13, at 513-15 (advocating a licensing system to allow the FCC to track BBSs and to provide the private sector with incentives to monitor).
220. *See* Cavazos, *supra* note 193, at 240; *Jensen, supra* note 18, at 233 ("[L]icensing requirements would cause hobbyist boards to go underground."); *Arnold, supra* note 1, at
ties have the incentive to use FCC requirements as a way to stifle or eliminate potentially socially desirable speech, and the FCC may ultimately promulgate content regulations. Further, the theoretical underpinnings supporting FCC regulation of BBSs seem shaky: BBS-based communication does not have sonic or visual interference and telephone line scarcity can be resolved given present technology. Additionally, there are limited circumstances where unconsenting users can be exposed to offensive materials because users must affirmatively seek out access to BBSs, which can institute screening mech-

3D. Historically, the initial intent behind licensing broadcasters was to promote radio expansion, but the opposite effect occurred. Pool, supra note 18, at 116.

221. See Firms Target Bulletin Boards to Stop Pirating of Software, San Jose Mercury News, Dec. 10, 1992, at 6G (describing how a software industry group has forced BBSs in Europe and Asia to shut down). Already corporations and private entities routinely monitor BBSs. See Harmon, New Legal Frontier, supra note 26, at A24 (explaining that many companies now covertly "lurk" on BBSs to find out what is being said about them); see also Schiffres, supra note 68, at 60 ("[All] the major toll carriers, as well as TRW, claim to monitor the boards closely [in 1985]."). For example, if given recourse through FCC regulation, these private entities may use the threat of a complaint to the FCC as leverage over BBSs who disseminate unflattering, but constitutionally protected, information.

222. See Karlin, supra note 30, at T6 (relating that an FCC regulation potentially holding sysops liable for "indecent" language transmitted across state lines caused two sysops in Alabama to restrict access to their BBS to in-state users); Uncapher, supra note 1, at 8 (explaining that, in 1991, the FCC cited numerous sysops because their computers, acting as gateways, automatically relayed messages that violated an FCC restriction on the use of amateur airwaves to promote business activities).

223. Three types of telephone line scarcity could affect BBSs. First, telephone line capacity could become a scarce resource. See Becker, Bulletin Board Operators, supra note 5, at 234 n.157. While the optimal method for upgrading the information-carrying capacity of telephone lines remains a hotly debated issue, there are a number of possible technological solutions to this constraint. See, e.g., Michael L. Dertouzos, Building the Information Marketplace, Tech. Rev., Jan. 1991, at 28, 32 (converting telephone lines from narrowband ISDN to broadband ISDN could result in an enormous increase in information carrying capacity).

Telephone numbers are the second scarce resource. See Jube Shiver Jr., Phone Numbers Grow Scarc in Information Age, L.A. Times, Feb. 8, 1993, at A1, A1 (without changes, the supply of telephone area codes will be exhausted by 1995); see also Eckhouse, supra note 70, at C7 (discussing how the proliferation of Internet accounts has consumed Internet addresses so rapidly that, unless standards are modified, the supply of Internet addresses will run out in 2003). Bellcore will introduce 640 new area codes by 1995 to alleviate the phone number constraint, but this is a temporary solution and does not resolve the capacity constraints in non-geographic specific prefixes such as the 800 and 900 phone numbers. Shiver, supra, at A11.

The third type of scarcity is telephone lines. For example, the ECHO BBS expanded so rapidly that it required every available line in the neighborhood. Stewart, supra note 72, at 155. This was resolved when the local phone company ran a separate cable just for ECHO. Id. However, even if telephone line or number scarcity becomes a binding constraint, market mechanisms may still be the optimal way to allocate them. See Pool, supra note 18, at 138-39.

224. See Jensen, supra note 18, at 239 (explaining that Pacifica concerns are not warranted in the BBS context because individuals must invest time and money to access BBSs...
RECOGNIZING LEGAL DIFFERENCES IN BBSs

While these conditions may change over time, until they do, there seems to be many dangers in, and few justifications for, FCC regulation of BBSs.

State-owned BBSs have different policy considerations. While there are many state-owned BBSs specifically designed for internal government uses or one-way communication, state-owned BBSs designed to facilitate public and interactive communication are difficult to distinguish from traditional public forums. Furthermore, users may reasonably expect significant user autonomy and liberal access. As state-owned BBSs proliferate, the courts should be vigilant about treating these BBSs as tools for tremendous communicative powers that should be protected and encouraged.

As a final consideration, there has been some discussion about whether legal doctrines applicable to BBSs should be rigid and well-articulated or determined on an ad hoc basis. The advantage to rigid rules is that they are predictable and can be applied consistently, which may result in judicial economy. One commentator argues that a federal solution is imperative, because state regulation will cause BBSs to locate in unregulated states. Another commentator has argued that the best approach to the choice of law problem in defamation cases is to create a federal common law. However, the problems these "global" solutions are trying to solve do not warrant such drastic measures; in fact, in some ways these "problems" work to the benefit of the technology. Although BBS users may be

and "very young" children will not be able to access computer messages); Miller, supra note 144, at 1192 (noting that BBSs are among the "least intrusive" media because they "require an initiating act or invitation to trigger transmission at home"). But see John Schwartz, Caution: Children at Play on Information Highway; Access to Adult Networks Holds Hazards, Wash. Post, Nov. 28, 1993, at A1 (describing the numerous ways that young children have been able to access adult materials on-line).

225. For example, users of a Sierra On-Line version of the adult interactive role-playing game Leisure Suit Larry must sign a statement that they are over eighteen years old. Markoff, The Latest Technology, supra note 16, at 5. However, the company's president wants the game to be "G-rated," and explains that, during the sex scenes, only the faces will be shown on the screen. Id.

226. See infra part V.

227. See Becker, Electronic Publishing, supra note 24, at 831.

228. See id. at 866 (arguing that all forms of electronic publishing should be treated as a single communications medium); Moore, Taming Cyberspace, supra note 28, at 749 ("We must address these issues in a more coherent, less ad hoc way.") (quoting computer science professor Lance Hoffman); cf. Charles, supra note 125, at 147-48 (outlining a very specific negligence standard for defamation liability to avoid the chilling effect of ad hoc balancing tests).

229. See Cutrera, Computer Networks, supra note 16, at 582; Faucher, supra note 38.


231. Faucher, supra note 38.
located nationwide, state regulation of BBSs might result in socially
desirable variations in government-mandated access, privacy and associ-
tional protections, or state-specific substantive laws. Therefore,
variations by state, despite the implicit confusion, may at this early
point in the growth of the technology prove to extend substantive and
procedural protections further than a homogenous federal approach.

More importantly, because the BBS industry is still maturing, ad
hoc determinations may defer the formation of difficult-to-change
rules until after the BBS technology is well-established, when the
true policy implications are clear. Rather than adopting hard-to-
change global rules, this Essay seeks to craft rules that are narrowly
tailored to the specific factual situations by focusing on the functional
capabilities of BBSs. If this approach is used, there is a reduced
chance that judges, trying to craft a decision that will account for all of

232. See supra text accompanying notes 136-42 (government mandated access); infra
part IV.A.2 (privacy and associational protections).

233. See M. ETHAN KATSH, THE ELECTRONIC MEDIA AND THE TRANSFORMATION OF
LAW 240 (1989) [hereinafter KATSH, THE ELECTRONIC MEDIA] (noting that the uses of a
new communication technology are often not apparent until the technology has prolifer-
ated); see also Johnson & Marks, supra note 88 (suggesting that, over time, custom and
technology will determine the appropriate legal principles); Perritt, Tort Liability, supra
note 126, at 95 (common law evolution is more flexible than administrative regulations); cf.
TRIBE, AMERICAN CONSTITUTIONAL LAW, supra note 41, at 1007 ("Novel communications
are pressed into service while still in their infancy, and the legal system's initial encounters
with these newborns often have a lasting influence."); Barlow, supra note 31, at 56 ("To-
day's heuristical answers of the moment become tomorrow's permanent institutions of
both law and expectation.").

For example, both telegraphy and computers were initially regulated as business enti-
ties, not as media, because the technology was so costly that businesses were the only
viable users. POOL, supra note 18, at 91; see Henry Beck, Control of, and Access to, On-
Line Computer Data Bases: Some First Amendment Issues in Videotext and Teletext, 5
COMM/ENT L.J. 1, 6-8 (1982) (discussing the evolution of the computer from a business
machine into a communications medium). As innovation reduced the cost of technology
and therefore increased its accessibility, these initial regulations became inadequate. For a
summary of significant changes in both the legal status and technology of BBSs between
1988 and 1992, see ROSE & WALLACE, supra note 1, at xiii, xix-xxii.

234. Cf. Perritt, Symposium, supra note 217 (looking at factual questions to resolve a
posed hypothetical); Miller, supra note 144, at 1199 & n.359 (explaining that sysops proba-
bly would prefer regulatory flexibility over legal certainty, even though each case would
then require fact-specific analysis to determine how the BBS was being used functionally).

Dec. 9, 1993), described supra note 30, is a prime example of the problems courts will
encounter should they fail to engage in fact-based analysis. In Frena, the court granted
plaintiff summary judgment on the copyright, trademark, and Lanham Act claims even
though the defendant sysop alleged that he was not aware that users had uploaded the
infringing photographs. Id. at *1. By granting summary judgment, the court essentially
held the sysop strictly liable—a very unfair result. A more appropriate approach would
have been to allow Frena to present evidence that he was merely an information dissemi-
nator and entitled to the defenses available to secondary publishers.
the variations in BBSs, will fashion sweeping rules that will prove difficult to dislodge after the technology has evolved.235

IV
Application of Existing Legal Doctrines to Specific BBS Functions

This part breaks BBSs down into their component functions to search for the appropriate legal analogies for each function. This function specific approach may seem odd, given that other communication technologies appear to “fit” in the publisher/broadcaster/common carrier legal tripartite. However, as has been shown, there is a sliding scale of editorial control and tort liability; if a media technology does not or cannot exercise its typical level of editorial control, then tort liabilities also abate. For example, in both Edwards and WDAY,236 the courts did not apply the prevailing defamation liability standard because the media did not exercise typical editorial control over the defamatory material.237 The versatility and multiple functions of BBSs, and other technologies such as cable television (which can act both as broadcasters and common carriers), stretch the usual boundaries because the level of editorial control can and should vary with the way the technology is being used. Therefore, function-specific legal rules for BBSs are not a radical jurisprudential approach, but rather explicitly reflect the fact that communications laws already adjust to the media’s specific function.

235. There is a real danger that civil liberties on BBSs will initially be accorded less protection. See Pool, supra note 18, at 250 (noting how “judges ha[ve] not got[ten] into the habit of being solicitous about guarding” freedom as new technologies have proliferated) (quoting Zechariah Chafee, Free Speech in the United States 381 (1941)); Rose & Wallace, supra note 1, at 101 (“Courts asked to apply older laws to new technologies will sometimes be afraid to [do so], throwing the ball back to the legislature to confirm that the same rights indeed apply to new technologies.”); Tribe, The Constitution in Cyberspace, supra note 36, at 21 (noting that recent cases regarding cable television make it appear “as if the Constitution had to be reinvented with the birth of each new technology”). Because cases decided today may greatly influence the course of future legal developments, see Pool, supra note 18, at 7; Tribe, American Constitutional Law, supra note 41, at 1003, it is important that early precedents in the BBS industry protect constitutional rights as much as possible.

236. See supra notes 161-62, 165-67; see also George E. Stevens & Harold M. Hoffman, Tort Liability for Defamation by Computer, 6 Rutgers J. Computers & L. 91, 94 n.18 (1977) (arguing that computer information processors should not be held liable for defamation if acting as conduits); McDaniel, supra note 7, at 819 (explaining that defamation liability requires some sort of publication function).

237. Cf. Miller, supra note 144, at 1188-89 (giving examples of how cable television laws reflect cable television’s hybrid of broadcasting and common carriage functions).
A. First and Fourth Amendment Cross-Functional Constitutional Considerations

Because the constitutional protections of the Fourth Amendment against search and seizure and of the First Amendment freedom to associate apply across all media technologies, these protections warrant special consideration and should apply to BBSs regardless of how the BBS is being used functionally.

1. Unreasonable Search and Seizure/Prior Restraint

Seizures of BBSs pose special problems because seizure eliminates the BBS's ability to communicate and, in essence, effects a prior restraint. Prior restraints are disfavored in all media (except common carriers): To obtain a prepublication restraint, the government must prove the "unprotected character of the particular speech with certainty," and "the irreparable nature of the harm that would occur if a prepublication restraint were not imposed, at least where timing is an important factor." The government should bear this burden if it wants to seize or otherwise preemptively restrain BBS-based communication.

Furthermore, if the government seizes a computer, it can search through the computer's entire hard drive, easily extending the search beyond the boundaries of the search warrant. Because such "shotgun" searches are disfavored, they should be deemed unconstitutional and courts should require significant specificity in granting and upholding search warrants related to computer seizures.

238. See Lawrence Edelman, Is This Man Invading Your Privacy? A Solution is Sought to Close Gap Between Technology and Law, Boston Globe, Nov. 20, 1990, at 25, 29 (quoting attorney Harvey Silverglate saying that the seizure of Steve Jackson's BBS computer and disks was functionally equivalent to the seizure of a printing press).

239. Telephone companies may terminate access of those who use obscene or indecent language, Pool, supra note 18, at 106, and the United States Postal Service may refuse to carry prohibited materials. Id. at 86-87.

240. Tribe, American Constitutional Law, supra note 41, at 1051.


242. One commentator has argued that because Congress failed to include BBSs in the relevant section of the Electronic Communication Privacy Act, see infra part IV.B.2, such evidence obtained unconstitutionally is not subject to exclusion at trial. See Cutrera, The Constitution in Cyberspace, supra note 195, at 152. This is unfortunate and warrants legislative remedy, given the significant opportunities for breaches of reasonable expectations of privacy.
2. **Associational Interests**

BBSs warrant consideration as private clubs, organized around mutual interests, that meet electronically. Indeed, electronic communication has increased group activity. Therefore, courts should carefully protect both the sysop’s right to associate and the user’s associational privacy.

As a general rule, sysops have the right to associate or not associate with whomever they choose. Because sysops may become liable for their users’ actions, sysops should have the right to choose their users and to deny access to users who harm others or reduce the quality of the BBS.

---

243. Katsh, *The First Amendment and Technological Change*, supra note 18, at 1474; see Arnold, *supra* note 1, at 3D (describing how sysops who were curious about their users invited the users to their house for a party); Christopher J. Galvin, *When Online Volunteermism Crosses Over*, COMPUTER MAG., June, 1993, at 12 (describing how CompuServe’s Judaism section of its Religious Forum adopted an official charity and raised over $4000 for this charity, including donations from “lurkers” who do not publicly participate in the Forum); Grimes, *supra* note 194, at 13 (Prodigy’s music discussion forum has arranged several social functions); Lawrence J. Magid, *Cyberspace! The Revolution in Online Service*, COMPUTER CURRENTS, July 20, 1993, at 24, 25 [hereinafter Magid, *Cyberspace!*] (“The WELL also encourages its members to get together—in real life—by sponsoring parties on a monthly basis.”); cf. Katsh, *The Electronic Media*, *supra* note 233, at 239 (noting that the ability to communicate efficiently with a large group of people has fostered the formation of global groups).


Rose and Wallace refer to one sysop who treats his BBS as his living room and his users as his guests:

> If the caller conducts himself in a civil manner and is considerate of others, he is permitted a lot of latitude in his behavior. If he is inconsiderate or does damaging things, he will be invited to leave, just as if he was really in the sysop’s living room and started hitting people or pouring beer on the furniture.

**Rose & Wallace, supra note 1, at 20; see also** Doll, *supra* note 75 (quoting a Ventura County sysop who also treats her BBS as her living room).

Some commentators have incorrectly asserted that sysops should not have meaningful First Amendment associational rights. *See, e.g.*, Di Lello, *supra* note 28, at 244. This can lead to the erroneous conclusion that a mandatory right to speak on BBSs will enhance, and not chill, the free marketplace of ideas. *See id.* Potential sysops, especially non-profit and non-commercial sysops, face scarcity in allocating capital (both time and financial resources) to the marketplace of ideas. Ignoring sysops’ associational freedom, especially in the face of potential tort or criminal liability, will make being a sysop less appealing at the margin and therefore will shift the sysop supply curve to the left. The result is higher costs and lower quantity supplied, shrinking the marketplace of ideas.
Nevertheless, states may partially circumscribe the sysop’s freedom to associate. The U.S. Supreme Court has upheld state legislation that compromises the right to associate or not associate if the state has a compelling state interest and chooses the least restrictive means to achieve the state’s end.\(^{246}\) Therefore, as a default, sysops may freely choose their members, but individual states, reflecting various state interests, may place some limitations on the sysop’s associational freedom.

The users also have important associational interests. For example, users may not be willing to associate with BBSs if sysops cannot keep BBS membership lists private.\(^{247}\) In *Gibson v. Florida Legislative Investigation Committee*,\(^{248}\) the U.S. Supreme Court held that state-mandated disclosure of membership lists requires that the state show a “substantial relation” between the membership list and a compelling state interest.\(^{249}\) Therefore, government mandated disclosure of membership lists should be strictly scrutinized.\(^{250}\)

More generally, the *Gibson* approach should apply not only to BBS membership lists, but also to disclosure of *all* the users’ actions on BBSs. Most BBS computers can and do track users’ electronic actions and can store and retrieve this information. In effect, users who assume that private electronic acts or statements are untraceable may find, over time, that their actions were tracked and can be disclosed through government intervention.\(^{251}\) Specifically, the historical ability to recreate users’ electronic movements and statements accurately, something the government cannot easily do in physical space, has the potential to lead to embarrassing or harmful disclosures.\(^{252}\) This ability of third parties to obtain information about users’ actions, espe-

---


\(^{247}\) See Charles, *supra* note 125, at 136. Some BBSs allow users to decide whether they want to be listed on membership directories available to other users. See *Becker, PC Communications*, *supra* note 3, at 235 (noting that CompuServe does not require users to join its publicly-accessible membership directory).


\(^{249}\) *Id.* at 546.

\(^{250}\) In the *Neidorf* case, see *supra* note 31, the Secret Service used membership on Neidorf’s mailing list as probable cause to issue a search warrant. See Cutrera, *The Constitution in Cyberspace*, *supra* note 195, at 157 & n.172. This sort of derivative use, without more evidence supporting suspicion, seems perilous in the face of *Gibson*’s associational privacy.


\(^{252}\) For example, the Air Force initiated court martial proceedings against Col. James A. Maxwell, Jr. for homosexual behavior after the Air Force learned that Maxwell had allegedly used America Online to find restaurants that cater to homosexuals and to
cially if users do not want such information to be known publicly, presents a real likelihood that users’ willingness to participate in BBSs will be inhibited. Therefore, as this monitoring becomes more commonplace, it may be appropriate to expand Gibson’s approach to include privacy of associational actions, or to combine associational privacy with the other zones of privacy created in the Fourth, Fifth, and Sixth Amendments and require strict scrutiny of government-mandated disclosure of this class of information.

However, even expanded First Amendment associational privacy will not prohibit private-party sysops from voluntarily disclosing membership lists or users’ actions to third parties. Perhaps, over time, sysops will voluntarily and routinely insert a non-disclosure or confidentiality provision in their contracts with users. An expansive approach to the tort of invasion of privacy may also inhibit sysop disclosure.

B. Function-Specific Analogies

In examining the different aspects of involvement that would warrant imposing sysop liability for users’ actions, the analysis ultimately depends on the level of sysop knowledge and control. For purposes of this part, it is necessary to establish working definitions of these terms.

“Knowledge.” If the sysop has actual knowledge of users’ actions, it is easier but not necessarily appropriate to impose liability. The more difficult inquiry surrounds the situation in which the sysop has imputed or constructive knowledge of users’ actions (i.e., the

---

253. These provisions may prove porous in application. For example, one sysop, a junior college professor, started men-only and women-only BBS conferences where the users agreed not to reveal the contents. Bulkeley, supra note 16, at B6. When one woman discovered that the male-only BBS contained an obscene message about her, she complained and the professor was forced to shut the BBSs down and was put on leave by the college. Id. While in this case the college was a state actor, the situation illustrates that other users, as well as sysops, pose a threat of disclosure despite non-disclosure or confidentiality provisions.

254. See Perritt, Tort Liability, supra note 126, at 108-10.

255. Cf. Restatement (Second) of Torts § 318 (1976) (articulating that chattel owners are not liable for the conduct of others when allowing others to use chattel if the owner (a) is not present, (b) cannot control the user, or (c) has no knowledge of the need to exercise such control).

256. Case law supports sysop liability if the sysop was “aware” that the defamatory material was available for distribution. Becker, Bulletin Board Operators, supra note 5, at 228. However, basing liability on knowledge, without also requiring the ability to control, could result in sysops being held strictly liable if they were unable to act.
sysop should have known). Because BBSs sometimes “operate without intervention for days or weeks at a time,” requiring all sysops to monitor their BBSs continually, even those operating “normally,” could be unduly burdensome. Therefore, for the purposes of this part, sysops do not have “knowledge” unless they have actual knowledge or were negligent in monitoring the contents of their BBS. Because negligence depends on the function being used and the sysop’s status (commercial versus hobbyist), and will evolve over time as the technology or industry practices change, an appropriate negligence standard would look at what a “reasonable sysop similarly situated” would have done given all the facts and circumstances. This may or may not include monitoring or other sorts of inquiry, depending on how the industry evolves.

“Control.” Sysops can exercise control over users’ actions in one of several ways: warning users that others may have posted harmful messages, instructing users not to harm others intentionally, reacting to users’ actions by removing harmful material, or preventing

257. Id. at 229-30; see Johnson & Marks, supra note 88, at 493 (“[I]n many communication systems, access to contents before ‘publication’ is a practical impossibility.”).
258. Loundy, supra note 45, at 103, 130, 136; Naughton, supra note 19, at 439.
259. Loundy, supra note 45, at 111; Johnson & Marks, supra note 88; Perritt, Symposium, supra note 217; cf. McDaniel, supra note 7, at 839 (arguing that all commercial BBSs should have a duty to inquire into information distributors’ credentials before granting access). But see Perritt, Tort Liability, supra note 126, at 103, 107 (explaining that any exercise of control may trigger imputation of knowledge).
260. Cf. Edward M. Di Cato, Operator Liability Associated with Maintaining a Computer Bulletin Board, 4 SOFTWARE L.J. 147, 156-57 (1990) (describing sysop “precautions,” which include: (a) requiring user registration, (b) physically separating user-uploaded material, (c) limiting the length of user messages, (d) prescreening messages, (e) setting time limits on length of user’s connect time, and (f) posting disclaimers).

One commentator suggested technology-based controls to replace sysop monitoring, including programming the computer to search for certain terms or information in certain formats and limiting the size of the messages or information the user can post on the BBS. See Gilbert, supra note 205, at 449-50.
261. See Don Oldenburg, Rights on the Line: Defining the Limits on the Networks, WASH. POST, Oct. 1, 1991, at E5 [hereinafter Oldenburg, Rights on the Line] (discussing the WELL’s Eros conference, where “[t]hose who enter are forewarned” that the conference is “pretty wide open to any of the most erotic ideas and writing you want to come up with”) (quoting Cliff Figallo, former director of the WELL).
262. See Reid, Nation’s Bulletin Board, supra note 92, at A4 (citing Phreakenstein’s Lair, a youth-oriented BBS, that warned users “[a]nyone leaving any message . . . dealing with breaking into computers, etc., will have their password ZAPPED!!!!!”).
263. Even if sysops exercise “reasonable care” in monitoring, offending or illegal messages can remain on the BBS for a day or longer. Sulski, supra note 32, at C17. On national and global network systems such as USENET, in which the message may be automatically stored and forwarded electronically between systems, the moderator (if there is one) may not be able to remove the message for days or even weeks. ROSE & WALLACE, supra note 1, at 15.
users from acting harmfully by prescreening their actions or denying access. For the purposes of this part, "editorial control" is defined as either (a) prescreening and exercising proactive control over the content of users' statements and actions, or (b) "customizing" the contents of the BBS, through the deletion of users' messages or the undoing of users' actions under a standard that is substantially more subjective than that required to avoid criminal or civil liability. However, editing and removing material not pertinent to the discussion is vital to avoid "clogged channels" and should not be considered editorial control.

I. Message Posting

Public message posting has proven the most difficult BBS function to analogize because it involves communication from many people to many people. It resembles the one-to-many communication of publication and broadcasting, not the one-to-one communication of telephones. The ability of any user to post messages at any time, however, differentiates the abilities of sysops from those of publishers

264. For example, CompuServe does not post messages that abuse others, "lessen the favorable experience of others using the service," or advertise other BBSs. Lewis, supra note 245, at 8 (quoting Dave Kissler, CompuServe spokesperson). This editorial policy employs somewhat amorphous standards (what activities "lessen the experience"?) which, if exercised extensively, probably should be considered editorial control. More refined standards, limiting CompuServe's intervention only to editing obscenity, redirecting off-topic messages to more appropriate discussion forums, or denying access to users who repeatedly post abusive messages, would clarify CompuServe's power to discriminate among content without triggering editorial control.

265. See Perritt, Tort Liability, supra note 126, at 140 ("It is unlikely that networks will survive where absolutely anyone can publish and users can read everything, deciding for themselves about value."); Cavazos, supra note 193, at 239 (describing the difficulties of maintaining a forum for children if users continually post "adult" messages). Indeed, with the opportunity for all users to post messages at their pleasure, many forums can be easily overrun by "junk postings" if sysops do not remove off-topic messages. Id. at 242; see Allen Lacy, A Gardener's World: When is Gardening a Subversive Act?, N.Y. TIMES, Jan. 31, 1991, at Cl (describing how a gardening forum on Prodigy drifted into discussions on the 1991 Persian Gulf War until Prodigy refused to post these off-topic messages). A similar problem can occur in software exchanges if, for example, users overrun the software utilities exchange with games postings.

266. See Lance Rose, The CompuServe Case—A Federal Court Recognizes Sysop Rights, BOARDWATCH MAG., Dec. 1991; Tribe, The Constitution in Cyberspace, supra note 36, at 18-19 (avoiding topic drift is analogous to the information organization and presentation undertaken by bookstores and does not represent editorial control).

267. See, e.g., Becker, Bulletin Board Operators, supra note 5, at 221.

268. This does not take into consideration, however, conference calls that allow communication between multiple, geographically-separated parties.
and broadcasters. 269 Indeed, the volume of information on BBSs often effectively prevents sysops from monitoring all postings. 270

In response to the easy access and high volume of public message posting, BBSs have sought different levels of control over, and responsibility for, users' messages. Prodigy states that it is responsible for its users' messages and therefore has the rights of a print publisher not to print every message submitted. 271 CompuServe and GENie remove obscene, illegal, or abusive messages as well as other messages based on user complaints. 272 The WELL's policy is that users own their words and are individually responsible for what they say. 273

Given that sysops have different objectives, the legal rules should allow sysops to choose the level of rights and responsibilities needed

269. See Cavazos, supra note 193, at 236-37; Computer Communications, supra note 125, at A6 ("There is no way we can patrol the boundaries of a multiple-gigabyte territory."); see also Di Lello, supra note 28, at 231 (explaining that Prodigy publishes on average approximately one message per subscriber every three weeks, which arguably no newspaper could do).

270. See Beall, supra note 13, at 505; see also Computer Communications, supra note 125, at A6 ("How can a network operator assume the obligations of a publisher . . . if network participants can post messages at will?"); see also Di Lello, supra note 28, at 231 (explaining how one sysop spent three hours a day reviewing messages); Andrew Pollack, Free-Speech Issues Surround Computer Bulletin Board Use, N.Y. TIMES, Nov. 12, 1984, at A1, A4 (concluding that sysops believe it would be "impossible to continue operating their boards if they had to monitor their boards at regular intervals").

271. Taylor, supra note 33, at C4 (quoting Martha Griffin, Prodigy spokesperson). Previously, Prodigy used prescreening to make its subscribers confident that everything on its BBS was suitable for every family member. See Moore, 1st Amendment, supra note 34, at 13. Prodigy no longer prescreens for content other than key words. Godwin, supra note 26. In response to the incident with the Anti-Defamation League, see supra note 28, Prodigy now censors all postings deemed "grossly repugnant to community standards," which includes anti-Semitic statements. John Schwartz, A Screenful of Venom, NEWSWEEK, Nov. 4, 1991, at 48.

One commentator has argued, unpersuasively, that Prodigy is not analogous to a newspaper or print publisher. See Di Lello, supra note 28, at 231-32. As shown in part III.A, media entities receive certain legal treatment based on a complex matrix of government interests and editorial control. If Prodigy exercises the type of editorial control similar to that of print publishers, other differences are irrelevant.

272. See Lewis, supra note 245, at 8; Taylor, supra note 33, at C4. To monitor activities on its different forums, GENie contracts with 120 people who have the power to remove messages. Sugawara, supra note 54, at A12. America Online only deletes about one message per year. Id.

273. Branscomb, supra note 38, at 156. However, this policy does not prevent the WELL from occasionally prohibiting some discussions or banning some users. Computer Communications, supra note 125, at A6; Schwartz, supra note 271, at 48. Contrast this with the positions of "self-styled 'First Amendment' BBS's . . . [that] deliberately refrain from interfering with their public message areas in the name of freedom of their callers' speech except in extreme cases where they fear serious legal problems." ROSE & WALLACE, supra note 1, at 9.
to carry them out effectively.\textsuperscript{274} From a policy perspective, sysops should be able to choose between being primary and secondary publishers so long as they accept the commensurate liability\textsuperscript{275} and the market is free so that users can choose between competing BBSs.\textsuperscript{276} Therefore, Prodigy can choose to become a primary publisher and gain the benefits of editorial discretion,\textsuperscript{277} but Prodigy will also be exposed to greater liability and possible consumer resistance. On the other hand, if sysops choose to become secondary publishers and intervene in users' actions only when they know that the actions are causing harm, the law should support this decision by granting them enhanced protection from liability in exchange for the free speech they promote.\textsuperscript{278}

Prodigy has argued that BBSs should be liable for users' statements only if the BBS "endorses" the users' statements,\textsuperscript{279} an argument that amounts to editorial control without legal liability for those statements Prodigy does not "endorse." This legal doctrine is perilous

\textsuperscript{274} Johnson \& Marks, \textit{supra} note 88, at 513-14 n.105; Henry H. Perritt, Jr., \textit{Dispute Resolution in Electronic Network Communities}, 38 \textit{VILL. L. REV.} 349 (1993) [hereinafter Perritt, \textit{Dispute Resolution}]; cf. Rose \& Wallace, \textit{supra} note 1, at 17 (advocating that USENET moderators should be able to choose how much control to exercise); Becker, \textit{Electronic Publishing}, \textit{supra} note 24, at 867-68 (arguing that BBSs that choose to become electronic publishers should have that right but should not dictate legal standards for those BBSs who choose not to undertake this role).

Note that other legal regimes allow individuals to choose their bundle of rights and obligations. For example, given a complicated set of tax, tort liability, and control issues, businesses can choose whether to organize as sole proprietorships, general partnerships, limited partnerships, corporations, or in some cases, limited liability companies. Similarly, given a complicated tradeoff between tort liability, control, and constitutional protections, sysops should have the opportunity to choose their bundle of rights and responsibilities.

\textsuperscript{275} While much of the focus has been on sysops' civil liability for users' statements, editorial control also can expose sysops acting as primary publishers to \textit{criminal} liability for obscenity. See \textit{supra} notes 207-13 and accompanying text.

\textsuperscript{276} See \textit{infra} part V.

\textsuperscript{277} These benefits are not limited strictly to control over users' actions. By adding value to the discussion through the exercise of editorial control, primary publishers may also claim a compilation copyright. See Rose \& Wallace, \textit{supra} note 1, at 49 (suggesting that sysops can claim a compilation copyright if they have "contributed enough . . . creative authorship" through active involvement in directing the discussion, such as the selection, arrangement, or coordination of postings). In contrast, sysops that strictly disseminate information have not added any originality to the information and cannot claim a compilation copyright. See generally Priscilla A. Walter \& Eric H. Sussman, \textit{Protecting Commercially Developed Information on the NREN}, \textit{COMPUTER LAW.}, Apr. 1993, at 1 (analyzing the application of Feist Publications, Inc. v. Rural Telephone Service Co., 499 U.S. 340 (1991), to electronic resources).

\textsuperscript{278} It would be unfair to hold these sysops liable because they do not exercise control, and it would be undesirable because BBSs serve an integral role in the dissemination and flow of information. See Rose \& Wallace, \textit{supra} note 1, at 11.

\textsuperscript{279} See Moore, \textit{Taming Cyberspace}, \textit{supra} note 28, at 748; see also Cutrera, \textit{Computer Networks}, \textit{supra} note 16, at 571 ("Prodigy wants to have its cake and eat it too.").
because it disengages the social costs from the private costs of Prodigy's actions. By exercising editorial control, Prodigy is making decisions that may impose costs on others. To make socially optimal decisions, however, Prodigy must internalize these social costs, which include the harm proximately caused as passed through by the tort system. If Prodigy is making decisions through the exercise of editorial control, but is not bearing tort liability for these actions, Prodigy will make its decisions based on its private costs, not the social costs, resulting in economic inefficiency. Therefore, Prodigy's "endorsement" or "control-without-liability" approach should be rejected because it prevents the tort system from effectively conveying the costs of poor social choices.

The non-interventionist approach is also problematic. If BBSs such as the WELL do not intervene at all, injured parties such as defamed individuals or copyright holders lack the ability to mitigate further damage.\textsuperscript{280} No other media, except common carriers, may knowingly allow harmful statements to be exchanged. However, unlike common carriers, such as telephone companies, removal of extant harmful materials from BBSs can prevent further harm without effecting a prior restraint or chilling constitutionally protected speech. Therefore, non-interventionist sysops, along with sysops who are categorized as secondary publishers, should have an obligation to remove tortious postings they know exist.\textsuperscript{281}

Some have argued that allowing sysops to choose their own level of rights and responsibilities will induce all sysops to "run [their] system[s] blindly,"\textsuperscript{282} effectively minimizing their contact with the BBS to reduce their exposure. This argument incorrectly presumes that the market will refuse to compensate the sysop for the sysop's greater ex-

\textsuperscript{280} See Becker, Bulletin Board Operators, supra note 5, at 229 (arguing that complete immunity will allow defamatory messages to be posted indefinitely). But see Cavazos, supra note 193, at 246-47 (concluding that BBSs allow a powerful and inexpensive right to reply to defamatory statements).

\textsuperscript{281} Rose & Wallace, supra note 1, at 9; Uncapher, supra note 1, at 14; cf. Sassan, supra note 47, at 840-43 (proposing that sysops have a duty to mitigate, which is fulfilled by removing the tortious posting after receiving notice and posting a retraction).

As discussed supra in part IV.A.2, at some point BBSs are more appropriately treated as associations rather than media entities. In those situations, it would be unfair to hold the BBS liable for its users' statements, just as it is unfair to hold an association liable for the statements of its members. Distinguishing between an association and a media entity is a very difficult line-drawing exercise; however, courts should continually consider the impact of potential rules on BBSs' associational interests.

\textsuperscript{282} Cavazos, supra note 193, at 242-43; accord Johnson & Marks, supra note 88; Miller, supra note 144, at 1196 (trying to read Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991), broadly in order to avoid this result). See infra text accompanying notes 306-10.
Further, this Essay suggests numerous places where the sysop cannot turn a blind eye, such as in the presence of postings the sysop knows are harmful. Therefore, since liability depends on whether the sysop exercises editorial control, sysops seeking application of the secondary publisher model will not be punished for, nor have incentives to refrain from, engaging in beneficial activities on BBSs.

Finally, state actors deserve a different analysis. To the extent that a state-owned BBS is intended to promote interactive communication and therefore acts as a limited public forum, the courts should strictly scrutinize content-based discrimination, and restrictions on access should be reasonable. On the other hand, a BBS not intended to promote interactive communication (i.e., BBSs that primarily transmit information one way to users) should be treated as a nonpublic forum, and the state should have wide latitude in its ability to restrict communication and user access. In either case, the state actors may have tort immunity by statute or common law.

2. Electronic Mail

Electronic mail differs from public message posting in that e-mail is one-to-one or one-to-many communication, in the sense that the sender specifically identifies one or more recipients. Congress has regulated e-mail somewhat, but these regulations do not protect e-mail as extensively as mail carried by the United States Postal Service. Sysops may not disclose electronic communications to third parties without permission or unless faced with valid search warrant, but

283. See Perritt, Dispute Resolution, supra note 274, at 356 ("Competitive forces will drive users to suppliers offering better terms."). Prodigy's volume of both users and subscribers has not translated into financial success. See Nikhil Hutheesing, The First Shall Be Last, FORBES, Oct. 25, 1993, at 220 (reporting that Prodigy has lost $1 billion cumulatively, $30 million in 1993 alone, and had to cut 25% of its staff). Nevertheless, Prodigy's difficulties are not necessarily due to its editorial policy; instead, it is plausible that its editorial policy has been instrumental in the success it has had.

Despite Prodigy's prominence, there also remains an immense segment of the market that does not exercise such extensive editorial control. See Naughton, supra note 19, at 434. For example, America Online, which has also experienced rapid growth in its user base and significant support on the stock market, removes on average only one message per year. See Sugawara, supra note 54, at A12.

284. See supra notes 184-86 and accompanying text.

285. See supra part III.A.2. Further, although the holding in Board of Education v. Pico, 457 U.S. 853 (1992), does not directly apply, the policies the Court articulated in Pico provide additional reasons for courts to strictly scrutinize content-discriminatory removals of postings. See supra text accompanying notes 153-54.


the statute does not prohibit sysops from reading correspondence, even if the e-mail is transmitted on company-owned BBSs and employers access employees' e-mail. Further, gateways can electronically copy e-mail as the gateway processes the information, and sysops and system administrators can access these back-ups.

Some BBSs have gone beyond the statute and instituted a policy against reading private e-mail. Others, acknowledging their power under the statute, have instituted a "no privacy" policy, stating that the sysop will read e-mail on occasion and, therefore, the user should not expect e-mail privacy.

Under the Electronic Communications Privacy Act, either approach is permissible but in the absence of a contractual agreement to the contrary, e-mail should be accorded the full legal protections afforded to physical mail. In particular, government entities should not have additional access to private e-mail simply because the information passes through a state-owned BBS; such power would give the government significantly greater access then it is allowed with physical

---

288. Id. § 2703. Under § 2707, the government has had to pay for wrongful seizure. See Steve Jackson Games, Inc. v. Secret Serv., 816 F. Supp. 432 (W.D. Tex. 1993) (awarding $1000 per plaintiff for seizure of e-mail messages); Victoria Slind-Flor, What is E-Mail Exactly?, NAT'L J., Nov. 25, 1991, at 3, 22 (noting the Riverside County coroner's office paid $1000 per individual, plus attorneys' fees, after it seized e-mail on a cryonics society's computer while searching for frozen bodies).

289. In fact, Congress recognizes that sysops can gain access to e-mail because the Electronic Communications Privacy Act allows third party disclosure of electronic communications to law enforcement officials if the sysop "inadvertently obtained" the communications. See 18 U.S.C § 2702(b)(6)(A) (1988); cf. Don J. DeBenedictis, E-Mail Snoops: Reading Others' Computer Messages May Be Against the Law, A.B.A. J., Sept. 1990, at 26 (discussing how the mayor of Colorado Springs systematically read backed-up personal e-mail sent between city council members without their knowledge).


292. See Markoff, The Latest Technology, supra note 16, at 5 (reporting that even though child pornography is being sent on America Online, the sysops do not monitor private e-mail); Moore, 1st Amendment, supra note 34, at 13 (stating that even when claiming the print publisher's power to edit public submissions, Prodigy claims that users' private e-mail is "strictly private" and not censored). But cf. Markoff, Home-Computer Network, supra note 33, at D5 (reporting that Prodigy restricted users from sending e-mail to system advertisers except to purchase or communicate about a specific order).

293. Meeks, supra note 213, at S14. However, even in such cases, users' e-mail privacy may be partially "protected by the sheer volume of messages." BECKER, PC COMMUNICATIONS, supra note 3, at 194.

mail protected by an envelope. In these situations, the state actor sysop should routinely destroy any back-ups or copies without any use or disclosure.

3. Real-Time Conferencing

Real-time conferencing is a many-to-many medium and is instantaneously interactive. When the sysop’s involvement is limited to merely providing the hardware, real-time conferencing is functionally equivalent to telephone conference calls. In these situations, the sysop should be treated like a common law common carrier. They should neither be liable for users’ actions, nor have the power to deny users access.

When sysops exercise some control over real-time conferences, it is inappropriate to allow them to claim the shield of either the common carrier or secondary publisher models. However, because the sysop’s control fluctuates as users enter or exit the conference or private rooms, to hold the sysop liable in these situations is problematic. Further, when users are interacting instantaneously, sysops cannot affirmatively control users. They can only react to problems by deleting messages once they have been transmitted and by ejecting users from the conference.

Holding sysops who exercise control on real-time conferences automatically liable for users’ actions would either inhibit sysops from trying to control interactive conferences or would force sysops to abandon the immediacy of conferencing for a system that permits sysops to screen communications prior to posting. The better approach is to treat real-time conferences as a committee meeting chaired by the sysop. In this analogy, the chairperson/sysop may exercise control by refusing to recognize certain members or ejecting troublesome users from the conference, but is not responsible for prescreening the opinions of the audience. This approach acknowledges the sysop’s limited control without forcing sysops to abandon the technology.

296. Because of the instantaneously interactive nature of real-time conferencing, these conferences should be treated differently than message posting. In message posting, the messages can persist for weeks, months, or even years; the sysop can prevent further harm by removing the message. See supra text accompanying note 280. On the other hand, in real-time conferencing, the information persists only a brief time during the interaction, so the sysop has limited power to prevent further harm from occurring after the fact.
297. See supra note 99.
4. Information Resources Dissemination

Several cases have addressed the legal status of on-line databases. The cases indicate that database creators are treated as primary publishers, while database disseminators are treated as secondary publishers.

In *Legi-Tech, Inc. v. Keiper*,\(^{298}\) the State of New York sold a computerized database of legislative materials. Legi-Tech, a for-profit company, sought unlimited access to the database to serve as source material for its own commercial computerized database. The state argued that, because it was not required to offer the computerized service, it could offer the service in a discriminatory way.\(^{299}\) The court rejected this argument and treated Legi-Tech as a press entity, holding that differential treatment of the press was unconstitutional unless there is some "special characteristic."\(^{300}\)

In *Daniel v. Dow Jones & Co.*,\(^{301}\) the plaintiff sued the database creator for negligently making false statements.\(^{302}\) New York common law had held news services not liable for negligently making false statements unless the parties had a special relationship.\(^{303}\) The court rejected plaintiff's claim because the parties did not have a special

---

\(^{298}\) 766 F.2d 728 (2d Cir. 1985).

\(^{299}\) *Id.* at 734. The court could have held that, under *Perry Education Association v. Perry Local Educators' Association*, 460 U.S. 37 (1983), the database was a nonpublic forum subject to reasonable regulation, including the refusal to provide unlimited access to a direct competitor. *See supra* part III.B; *cf. Mayo v. United States Gov't Printing Office*, 9 F.3d 1450 (9th Cir. 1993) (denying a BBS's request for free access to electronic slip opinions under a common law "right to inspect" public records). The court's approach, relying on special rights given to the press, seems less persuasive after the rejection of a media/nonmedia distinction for defamation purposes in *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749 (1985).


\(^{302}\) Plaintiff was a subscriber and a securities investor. Defendant provided allegedly misleading information, because it stated prices in dollars without specifying whether the dollars were American or Canadian.

relationship beyond the ordinary buyer/seller relationship: "There is no functional difference between defendant's service and the distribution of a moderate circulation newspaper or subscription newsletter. . . . [I]f the substance of a transaction has not changed, new technology does not require a new legal rule merely because of its novelty." Therefore, the court's holding that computerized on-line databases could not be held liable is predicated on the fact that newspapers could not be held liable under the common law or under the First Amendment for negligent omissions.

In contrast, in Cubby, Inc. v. CompuServe, Inc., the court analyzed CompuServe's liability for defamation differently because CompuServe was the electronic distributor of a magazine, not the author. CompuServe contracted with Cameron Communications, Inc., an organization wholly independent from CompuServe, to have Cameron manage the "Journalism Forum" subject to standards developed by CompuServe. Don Fitzpatrick Associates ("DFA") contracted with Cameron to provide a daily newsletter to the Journalism Forum entitled Rumorville USA. Plaintiffs initiated a rival newsletter and sued for libel, business disparagement, and unfair competition based on statements Rumorville made about plaintiffs.

The court enumerated the restraints on CompuServe's control over Rumorville: (1) CompuServe users subscribed directly with DFA for Rumorville; (2) DFA uploaded Rumorville to CompuServe's computers without giving CompuServe opportunity to review it; (3) CompuServe received no revenues directly from users' subscription to Rumorville; and (4) CompuServe claimed that it had not received any complaints about the magazine.

304. Id. at 337-38.
305. Noting that the U.S. Supreme Court in Greenmoss Builders largely collapsed the media/nonmedia distinction, the court treated the "wire service" as a media defendant. Id. at 339-40. As a result, "[n]ews services . . . such as defendant's computerized database, are instruments for the free flow of all forms of information, and should be treated as unquestionably within the First Amendment's guarantee of freedom of the press." Id. at 340.
307. On some BBSs, discussion forums are managed or "referred" by third parties to minimize "junk" postings and increase the level and quality of discussion on the forum. See Rose & Wallace, supra note 1, at 14-17 (addressing some of the rights and responsibilities of moderators on USENET); Oldenburg, Rights on the Line, supra note 261, at E5 (noting the importance of a moderator to keep conversations focused). CompuServe uses outside independent forum managers (sysops) for each of its forums. Becker, PC Communications, supra note 3, at 221.
308. 776 F. Supp. at 137. Future courts should look at these four factors in applying Cubby. Because CompuServe's structure is unique, however, courts should not necessarily
Plaintiffs claimed that CompuServe was a publisher. CompuServe moved for summary judgment, claiming that it acted as a news distributor. Following Smith v. California, the Court held:

CompuServe[... is in essence an electronic, for-profit library that carries a vast number of publications and collects usage and membership fees from its subscribers in return for access to the publications. [... While CompuServe may decline to carry a given publication altogether, in reality, once it does decide to carry a publication, it will have little or no editorial control over that publication’s contents. This is especially so when CompuServe carries the publication as part of a forum that is managed by a company unrelated to CompuServe. [... CompuServe has no more editorial control over [Rumorville] 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.

Therefore, recognizing CompuServe’s nonexistent editorial control over the defamatory material, the Cubby court held that CompuServe warranted more favorable legal treatment as a secondary publisher.

Collectively, the case holdings indicate that BBSs/sysops that develop electronic databases will be treated as primary publishers, while BBSs/sysops that act as a “conduit” for other database developers or publishers will be treated as secondary publishers. From a policy perspective, these outcomes are appropriate. Giving sysops the opportunity to shield themselves from liability (by acting as an information disseminator) allows sysops to provide additional information services and increases overall access to information. On the other hand, sysops that want to be primary publishers will have the power to do so, but at the cost of greater exposure to tort (and possibly contract) liability.

require all four factors to find that BBSs functioning as information databases are secondary publishers.


310. 776 F. Supp. at 140 (emphasis added). The court continued that imposing a lower standard of liability on an “electronic news distributor such as CompuServe” would unduly burden the free flow of information. Id.

311. A sysop may want to be considered a primary publisher to obtain, among other things, enhanced protection from search and seizure, compilation copyrights, or additional access to information available to press entities. For example, Delphi, a national BBS, offers a service where it analyzes, collects, and makes available to its users information resources from the Internet. Magid, Cyberspace!, supra note 243, at 26. Essentially, by performing this service, Delphi acts as a republisher, for which it presumably receives additional revenues and/or market share to compensate for the additional liability.

312. One commentator has argued, unpersuasively, that the Cubby holding applies only to CompuServe, and not to Prodigy, because CompuServe is functionally equivalent to a bookstore while Prodigy is designed for shopping and more functionally equivalent to a shopping mall. See Di Lello, supra note 28, at 228-29. Putting aside the obvious (that even bookstores are designed for shopping), the commentator misses the point of his “functional
5. **Software Distribution and Commercial Services**

Software dissemination on BBSs poses two general problems. First, software exchanges are many-to-many forums, and the volume of software uploaded makes monitoring by the sysops difficult. Second, in providing software or other commercial services such as information storage or electronic shopping, BBSs are essentially selling products. Therefore, in some respects, sysops act as vendors or distributors.

In these situations, the allocation of tort liability should turn on whether the BBS is a vendor. In other words, commercial BBSs that tout their reputation for software files and are perceived as software distributors should be treated as such for tort purposes, as should those BBSs that provide other types of commercial services. Liability imposes greater responsibility on these BBSs and, to a lesser extent, all commercial BBSs (which, even if not vendors, will have to obtain insurance or raise fees to reflect the costs of possible liability), but this liability is appropriately borne by the users through the BBSs' fees. However, because these sysops should have a reasonable oppor-

---

313. See Lance Rose, *All the News That's Fair to Use*, BOARDWATCH MAG., May, 1992; cf. Di Cato, supra note 260, at 158 (acknowledging the potential need to distinguish between commercial and free BBSs). On one level, the result in Playboy Enterprises, Inc. v. Frena, No. 93-489-CIV-J-20, 1993 WL 522892 (M.D. Fla. Dec. 9, 1993), in which the court found the sysop liable for digitized *Playboy* photos uploaded by users, can be explained by this approach. Although the *Frena* court did not explain why it considered the sysop responsible for his users' actions, the fact that the BBS was commercial and received revenues in part because of its photo libraries suggests one reason why the court was comfortable imposing liability. See id. at *11 (analyzing the "reverse passing off" issue by focusing on the treatment of plaintiff's "products").

The distinction between commercial and free BBSs for the purposes of software downloading has been proposed in other contexts. See Barbara E. McMullen & John F. McMullen, *Confusion Reigns on NY State "Download" Tax*, NEWSBYTES, Sept. 12, 1991, available in WESTLAW, Comp-ASAP file (noting that a New York sales tax law appeared to require sysops to remit sales taxes on downloaded software but was interpreted not to include free BBSs); cf. Cavazos, supra note 193, at 239 n.48 (noting that Southwestern Bell charges noncommercial telephone rates to Texas BBSs that have fewer than three incoming lines).
tunity to remove uploaded copyrighted software, the liability standard should be negligence, \textsuperscript{314} not strict liability.

In contrast, free BBSs cannot pass on the cost of tort liability to their users. Therefore, in allocating losses between these sysops and their user, the tort laws should favor the sysops. \textsuperscript{315} Indeed, legal solicitude toward services like software distribution on free BBSs is especially important given that users can obtain freeware and shareware on these BBSs, which, over time, could increase access to computer technology by the disenfranchised.

However, in the case of software distribution, because copyright violations harm third parties, even free BBSs must bear some responsibility. Since it is difficult for sysops to monitor software uploading, they should not be liable unless they have knowledge of the copyright violation \textit{and} failed to exercise control by removing the copyrighted software. \textsuperscript{316} With this standard, copyright holders will be able to mitigate their damages, \textsuperscript{317} but sysops of free BBSs will receive ample protection from liability.

6. \textit{Gateways}

Computers acting as gateways by definition do not have either knowledge or control of the information being transmitted. In this respect, gateways act as common law common carriers and it would be unreasonable to hold the BBS or network liable for users' actions, \textsuperscript{318}

\textsuperscript{314} The negligence standard should apply, for example, if the sysop failed to remove the copyrighted posting after receiving actual knowledge or within a reasonable time (as determined by sysops similarly situated). \textit{See supra} text accompanying notes 258-59.

\textsuperscript{315} For example, users should have the burden to check the software for viruses. Not only can users easily check for viruses, but users should also know of the need to do so. \textit{See} BECKER, \textit{PC COMMUNICATIONS}, \textit{supra} note 3, at 126.

\textsuperscript{316} \textit{Cf.} Di Cato, \textit{supra} note 260, at 155-56 (advocating that only sysops who act intentionally or grossly negligently be liable for the illegal distribution of copyrighted software).

\textsuperscript{317} However, copyright holders will have some responsibility to monitor BBSs and to point out violations to the sysop. This obligation may be onerous but no more so than exists in physical space.

\textsuperscript{318} This is essentially the argument the court accepted in Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991). Rose and Wallace suggest that, because sysops can decide not to act as a gateway, some liability might accrue if the BBS acts as a gateway to a discussion forum or file exchange that repeatedly engages in tortious or illegal conduct. \textit{R}OSE \& \textit{W}ALLACE, \textit{supra} note 1, at 15-16; \textit{see also} McDaniel, \textit{supra} note 7, at 839 (arguing essentially the same in the information services context). The \textit{Cubby} court recognized this possibility but did not address it directly. \textit{See supra} text accompanying note 310.

As a result, to clarify the lack of liability, some commentators have proposed an "Electronic Communications Forwarding Act" which would absolve from liability entities that only forward communications. \textit{See} Johnson \& Marks, \textit{supra} note 88, at 510-11; Perritt, \textit{Symposium}, \textit{supra} note 217, at 343 (concluding remarks of Shari Steele of the Electronic Frontier Foundation).
for much the same reasons as those articulated in *Smith* and *Pico*. In contrast, if liability is imposed, it will encourage information conduits to censor or reduce the flow of information.\(^{319}\) However, as common carriers, the BBS gateways may not discriminate either in user access or in transmitting the information. This lack of discrimination will be essential to the imminent development of a single national information network, which should be required to carry any and all BBSs that choose to affiliate with that network.\(^{320}\)

V

Conclusions

By examining computer bulletin boards in their relevant constituent components, this Essay has sought to show that existing legal precedents can be used on a function-specific basis to protect the rights of both sysops and users and to further important policies.\(^{321}\) As legal fact finders analyze BBSs, judicious use of existing legal precedents can promote the development of the BBS industry.

However, this Essay has also argued that sysop liability should depend on the amount of knowledge and control a sysop exercises for the specific function in question. On a function-specific basis, sysops can choose the level of knowledge and control they want, with the concomitant rights and responsibilities.\(^{322}\)

---

319. *See* Perritt, *Symposium*, *supra* note 217; *cf.* Johnson & Marks, *supra* note 88 (arguing that a duty to monitor will reduce the number of sysops).


322. *Rose & Wallace*, *supra* note 1, at 20 ("[S]ysops [can] adjust the amount of freedom and power they give to callers, and the amount of legal risk they can take on."); *accord* Perritt, *Tort Liability*, *supra* note 126, at 66 (emphasizing the sysop’s choice in control and risk); McDaniel, *supra* note 7, at 785; Meeks, *supra* note 213, at S14 ("[S]ysops have the right to run their systems any way they see fit."). However, allowing sysops to exercise editorial discretion allows private parties to inhibit free speech. In critiquing Prodigy’s actions, Jerry Berman, formerly of the ACLU, said: "[W]e should be concerned if systems such as Prodigy become the rule. Instead of expanding speech, we’ll have electronic forums that are quite limited." *Markoff, Home Computer Network*, *supra* note 33, at D5; *accord* Di Lello, *supra* note 28, at 245-46; *cf.* Tribe, *American Constitutional Law*, *supra* note 41, at 1009 n.78 ("[W]e cannot depend upon those who own and control the new media to resolve the critical issues of access and availability in a publicly-responsible manner."). To avoid excessive private-sector stifling of free speech, Berman suggests that either the market must provide significant meaningful choices or Congress must regulate. *See* Taylor, *supra* note 33, at 4.
As a default state of the law, this legal conclusion may not be particularly significant if sysops and users choose to resolve these issues contractually. So long as the BBS industry remains characterized by easy entry and exit, sysops and users should have the ability to negotiate any one of the myriad of contractual allocations of rights and responsibilities available, if the contractual resolutions sufficiently protect the interests of third parties. With a competitive free market and proper cost pass-through, users will provide appropriate market incentives to allow the BBS industry to achieve a free market equilibrium without extensive government intervention, regulation,

323. See Oldenburg, The Law, supra note 45, at E5 (quoting Lance Rose). In fact some commentators have suggested that contracts and not statutes should currently be the primary way to govern computer communications. See, e.g., Johnson & Marks, supra note 88.

However, the formation of an industry group could restrict users' power to contract freely. "[T]he most comprehensive censorship [in broadcasting] . . . consists of elaborate systems of 'self-regulation' which the broadcast industry imposes on itself . . . ." TRIBE, AMERICAN CONSTITUTIONAL LAW, supra note 41, at 1002-03 n.35; see POOL, supra note 18, at 121 (positing that the initial censorship in radio broadcasting was driven by the attitude "censor ourselves so the government will not"); cf. Charles, supra note 125, at 149 (arguing that sysops could avoid court intervention by forming an industry group to develop industry-wide rules). In fact, in 1984, the New York Sysops Association, a BBS industry group, pressured sysops to restrict the use of BBSs for illegal activity. See McGill, supra note 6, at B5; see also Kahn, supra note 168, at 17-18 (describing the standards for sysops articulated by a BBS user group).

However, even if industry-wide standards emerge, this should not override the right of parties to form enforceable contracts in cyberspace. In fact, robust contract law is an essential component of a properly functioning free market. Perritt, Dispute Resolution, supra note 274. However, sysops might standardize contracts of adhesion, which bind users to statements that appear on the screen for a few seconds and provide one-way protection for the sysop only. See McDaniel, supra note 7, at 837-38; see also Di Lello, supra note 28, at 232 (arguing that Prodigy's contract is adhesive). These contracts should be voidable just as they would be in physical space.

324. Some commentators argue that sysop liability should be exclusively governed by the user/sysop contract. See, e.g., Johnson & Marks, supra note 88; Perritt, Dispute Resolution, supra note 274, at 396-97 (proposing a statute where, if sysops post "Terms of Service," they shall not be liable to "any person" for injury caused by the users); Cutrera, Computer Networks, supra note 16, at 582-83. This is unrealistic, as there always will be cases where the contract is silent on the key issue or where no contract exists. More importantly, this could lead to a contractual version of Prodigy's current approach of exercising editorial control, but absolving itself of all liability for its actions. As noted supra in the text accompanying note 279, this distorts the free market by uncoupling Prodigy's private costs from the implicit social costs of its actions. Therefore, while contractual allocations are desirable and should be encouraged, courts should disallow provisions that, based on existing constitutional jurisprudence, do not properly allocate social costs.

325. See supra part IV.B.

326. See Perritt, Tort Liability, supra note 126, at 137-38 (market competition achieves all policy goals); Kapor, supra note 22, at 162 ("[M]arket competition is the most efficient means of ensuring that needs of network users will be met."); cf. Moore, 1st Amendment, supra note 34, at 13 (arguing that if users want "uninhibited, titillating conversation," they can subscribe to BBSs other than Prodigy).
or judicial overreaching. Given the current robustness and dynamism of the marketplace, there are strong indicia that the free market is currently functioning normally.

Of course, as with any emergent technology, future situations could undermine the assumptions underlying the free market. For example, this free marketplace analysis assumes that users provide the primary source of benefits. If user revenues become less important to sysops than other revenue sources, then BBSs will cater to these other sources, not to users. Advertiser-driven content regulation by BBSs will not be a problem if noncommercial BBSs retain their vitality; however, should Prodigy's model of advertising on every screen become more prevalent, then the free market analysis must be retooled to examine sysops' relationship with advertisers.

More likely, should the BBS industry consolidate to the point that individual BBSs command market power, or should the BBS

---

327. Government regulation of media is a last recourse. Pool, supra note 18, at 246; see Kapor, supra note 22, at 162 (seeking to limit government subsidization or regulation because such intervention can lead to content-based discrimination).

328. See supra text accompanying notes 10-15; see also Johnson & Marks, supra note 88, at 504 ("The ease with which sysops can develop a system, and the relative ease with which consumers can access the service, are leading to a drastic increase in both the number of systems available to the consumers and in the usage of such systems."); Cutrera, Computer Networks, supra note 16, at 573 ("The cost of starting a bulletin board is so low that a thriving, competitive market is developing.") (footnote omitted); Naughton, supra note 19, at 434-35. However there are some transaction costs that may pervert the free market. See Perritt, Dispute Resolution, supra note 274, at 357 (citing when there is "significant detrimental reliance on the network's service terms"); see also Richard Core, Prodigy Readmits Foe of Shock Jock, L.A. Times, Oct. 2, 1993, Orange County edition, at B4 (reporting that a Prodigy user who was kicked off the system for personal attacks against Howard Stern sued Prodigy in small claims court for the costs of switching to another BBS). While the large numbers of unsubscribed potential customers keeps pressure on BBSs, as the market becomes significantly more mature, these switching costs may hinder the vitality of the free market.

329. See Tribe, American Constitutional Law, supra note 41, at 1002-03 n.35 (noting that advertising revenues engender adherence to broadcasters' self-imposed censorship guidelines in order to keep Nielsen ratings high and to avoid offending advertisers).

330. Prodigy apparently has failed to raise significant revenues from its advertisers, however, and has changed its pricing structure to derive more revenues (and a larger percentage of revenues) from users. See Kathleen Creighton, The End of BBSing on Prodigy?, Micrometimes, May 31, 1993, at 114, 186.

331. See Perritt, Tort Liability, supra note 126, at 134 (arguing that private electronic networks should be subject to mandatory access only if the network has a monopoly position that precludes access); see also Miller, supra note 144, at 1196.

The idea that individual BBSs command market power is not inconceivable. See Di Lello, supra note 28, at 245-46 (presuming that Prodigy, and its censorship model, will dominate the market). But see Harmon, Price War, supra note 60, at D2 (noting its significant financial problems, some have speculated that Prodigy will not survive).

However, the Internet is consolidating market power. Because the Internet is the largest and most global network, users are consolidating on BBSs that connect to the In-
industry become an indispensable link in the nation’s communications chain, then we can anticipate that the current legal doctrines will be insufficient to meet our policy objectives. At that time, it may be appropriate to reevaluate government intervention\(^3\) or the identification of these BBSs as state actors,\(^3\) as these actions may prove best to protect the rights and interests of sysops, users, and third parties.

\(^3\) Laurence Tribe has argued that the size of some electronic networks has created “virtual ‘governments’” that create their own access policies and operate internationally. Oldenburg, *The Law,* supra note 45, at E5. Therefore, these networks “may be outgrowing their private status and ripening for regulation.” *Id.*; *see* Di Lello, *supra* note 28, at 231, 241 (arguing that “the [present] danger of market power and monopoly are considerable” and arguing for federal regulation of commercial BBSs); Perritt, *Tort Liability,* *supra* note 126, at 149 (arguing that the FCC should begin an inquiry into network denials of access).

\(^3\) See Naughton, *supra* note 19, at 434-35 & n.150 (arguing that if the market becomes concentrated, BBSs should be considered under the cases allowing users the right to access private property).