Computer Bulletin Board Technology:
Sysop Control and Liability in a Decentralized Information Economy
by Eric Schlachter

ABSTRACT

The explosive growth of computer bulletin board technology poses imminent legal and cultural chaos. The multiple functions of computer bulletin boards will affect the way that we communicate and affiliate with others, and problems arise in determining system operators' responsibility for what happens on their boards. This paper uses different paradigms in considering system operator ("sysop") liability: in some cases, it is appropriate to assign liability when the sysop acts as a co-conspirator; in other cases, liability should accrue when the sysop exercises editorial control. Ultimately, if given the benefit of applicable constitutional procedural protections, either paradigm can lead to appropriate cost internalization, which in turn can help sysops make decisions that will support the proper functioning of the free market.

I. WHAT CAN THIS TECHNOLOGY DO, ANYWAY?

Computer bulletin board technology, as it evolves, is collapsing previously distinct categories.[1] To reflect the technological convergence of capabilities, I define "computer bulletin board" (or "BBS") technology to include the following technologies: computer bulletin boards, electronic bulletin boards, network nodes, on-line services, information services, videotex services, electronic publishers, electronic networks, and electronic mail systems.

This technology, defined broadly, has many applications. A temporally comprehensive list includes the following functions:

Electronic user-to-user communication, including bulletin board postings (i.e., many-to-many communication through centralized channels), private electronic mail (direct user-to-user communication), and real-time "chats" (like telephone conference calls, except anyone can join in).

Access to information databases and electronic information publishing, including user-to-system interaction such as the dissemination of credit information or stock quotes, where the user interacts directly with the computer. However, this also includes the FTP and "gopher" functions, where users can browse and retrieve on-line libraries.

Electronic commerce, ranging from on-line travel reservations and stock brokerage to ordering Godiva chocolates to electronic classified advertisements.

Information storage, where the user stores information on the system computer.

Software exchange, where users upload or download freeware, shareware, digitized art and sound, and other forms of computer-usable files and programs.

Gateways. Many bulletin boards provide connections, sometimes transparent, to other services or electronic networks. The ability to spin webs of networked BBSs is among one of the most exciting features of this technology and is at the heart of the oft-discussed information superhighway.

II. THE SOCIAL BENEFITS ACCRUING FROM COMPUTER BULLETIN BOARD TECHNOLOGY

The speed and cost-effectiveness of computer bulletin board technology in performing the above functions has already resulted in numerous important benefits to society:

Increased group activity. Ithiel de Sola Pool has noted that group formation is no longer geographically based;[2] rather, it can transcend geographic regions and segments of society. Thus, BBS technology allows people with oblique and highly specialized interests to affiliate together without the high search costs prohibiting such physical world affiliations. For example, those people devoted to chicken beaks can find each other and ruminate on the subject to their hearts' content.

On-line altruism. An amazing on-line phenomenon has been the emergence of electronic communities whose norms diverge from "rational maximizer" economic theory. Cyberspace has seen numerous displays of altruism, despite social anonymity (i.e., a minimal chance of future on-line encounters), where users help out other users with their time and sometimes their extremely valuable expertise.[3] Indeed, this on-line altruism overcomes the free rider problem and creates public goods *without* government intervention.

Electronic Democracy. The ability of electronic networks to subvert hierarchies has produced opportunities for citizens to access politicians more directly. Although President Clinton and Vice President Gore are newcomers to the Internet, for years politicians have had bulletin boards for constituents that have allowed otherwise silent constituents to participate in the political process. As a related result, government has gotten closer to the people: bulletin boards in states such as Montana and Hawaii and in the City of Santa Monica permit constituents to reach government services on-line. Many courts now make their opinions available through BBSs (though, sadly, not all of these are publicly accessible) and numerous people have sought to make legislative materials available on-line.

The impact of BBS technology on political developments has significant ramifications. Electronic networks distribute power decentrally, allowing information to bypass hierarchies and central controls. When information seeks to be free, so do the people.

The Great Equalizer? Currently, electronic communication is stripped of most of the typical visual cues we otherwise use to make selections and discriminations. Recipients of my electronic product need not know my ethnicity, socio-economic status, or sexual preference. As a result, we are all given an opportunity to stand on the strength of our words; a heavy burden placed on mere words, but an only slightly-tilted playing field nonetheless.

III. ALLOCATING LIABILITY BETWEEN SYSOPS, USERS, AND THIRD PARTIES

Jon Katz of *Rolling Stone* has suggested that BBS technology eliminates the need for "gatekeepers."[4] Where our activities, and to some extent our thoughts, have historically been channeled through physical bottlenecks such as newspapers or broadcasters (where there were serious barriers to entry), now users have decentralized power to reach the entire computing world. This decentralized power has the potential to increase both the number and scope of criminal and tortious wrongs committed. Our challenge is to circumscribe the wrongs as narrowly as possible while retaining the social benefits of the technology.

Intra-party allocations

Most problems between users and sysops do not materially differ from problems experienced in physical space. For example, sysops can disseminate defective or virus-infected software or faulty information through system databases, can misdirect communications (such as delivering a message to the wrong person) or invade a user's privacy by embarrassing disclosures, or damage users' data stored on the sysop's hard drive. For the most part, these types of problems can be and are addressed in the parties' contract.[5] However, even if not addressed by contract, these types of problems do not require new laws; fact-specific jurisprudence can apply existing rules effectively to the electronic context.

Many people have taken issue with contractual allocations of power between sysops and users, noting that sysops have too much power to censor, such as Prodigy's ejection of 12 users who complained too boisterously about Prodigy's imposition of a per-email charge. While private discrimination and censorship do pose dangers, freedom of private action is not unique: numerous cases

ISBN: 0-7803-0932-4/93/$3.00©1993IEEE

limit government intrusion into private associations and private property used for communications purposes.[6] Further, a robust free market obviates the need to limit the freedom to contract; users discriminated against have had no problem fleeing BBSs such as Prodigy and reconvening on electronic venues more suitable to their interests. Therefore, until the free market no longer supports freedom of contract, we do not need government regulation to allocate rights and responsibilities strictly between users and sysops.

Dangers Posed to Third Parties

Although intra-party allocations are important, the real challenges BBSs pose to society radiate from users' ability to harm third parties. At the crux of the matter is when the sysop has become part of the causal chain. The way we draw the line has significant impacts on what sysops can do and whether or not they will choose to remain part of the industry.

The Facilitator Problem: Stolen Information, Copyright Violations, and the Distribution of Harmful Agents such as Viruses.

Stolen information such as computer passwords and telephone credit card numbers have played a significant role in the development of the industry. Indeed, the 1984 Thomas Tcimpidis incident triggered commentators and scholars to discuss the difficult legal issues posed by BBSs.[7] Laws now assign liability to the person who steals the information,[8] but considerable confusion remains about when sysops are liable for the presence of this stolen information on their BBSs. At some point, society's interests in stopping the flow of stolen information requires us to place some burdens on the sysop, but where? Given the volume of information uploaded and downloaded on some BBSs daily, it is almost logistically impossible for most sysops to sift through all the postings to determine the presence of stolen information.

The analysis for copyrighted software and transmission of viruses follows the same kind of reasoning. Software postings can occupy gigabytes of storage space, and most BBSs allow users to upload and download as they please. Further, except for obvious cases, sysops have great difficulty knowing whether or not software is copyrighted or infected.

Deciding when sysops are liable for these types of users' actions has profound ramifications. If we want to favor the interests of the telephone charge card holder, copyright holder, or subsequent infected party, we could hold sysops absolutely liable for the presence of stolen information or pirated or infected software on their BBS. Of course, this favoritism has a price: heavy prescreening (which is probably not foolproof and which would probably lead to censorship erring on the conservative side), high user fees to cover insurance, or the disappearance of sysops from the industry.

An alternative, and I think superior, approach treats the offending user as the criminal actor, and then look for evidence that the sysop is a co-conspirator or criminal facilitator. In either case, the sysop must have some specific criminal intent before being held criminally liable. Ignorance should not satisfy the definition of intent unless the ignorance is willful (i.e., "I didn't look because I had my doubts and I didn't want to know."). With this standard, sysops can operate with the default presumption that everything is OK, and the sysop will have obligations to act only if the sysop receives or encounters some indication that criminal activity is taking place.

Even if the sysop is not criminally liable, injured third parties still have recourse in tort. Tort liability accrues only if the sysop has a duty to the third party and failed to exercise due care. While defining duties is often tautological (i.e., there is a duty because we want there to be a duty), no one knows what constitutes the exercise of due care. Although some have argued for very precise negligence standards[9] to remove uncertainty, the technology is so fluid and the applications so varied that I believe comprehensive and workable standards are not yet tenable. However, some guidelines could be established that clarify what would essentially be a facts and circumstances test. For example, failure to monitor should not be per se negligence; failure to remove illegal or copyrighted postings within a reasonable period after receiving *actual* (not constructive) notice of the illegal or copyrighted nature of the posting should be deemed negligence. Thus, guidelines that set only outer boundaries are probably the best bet in the current dynamic industry.

The Editorial Control Problem: Defamation, Obscenity, Copyright Protection, and Enhanced Press Powers.

In physical space, legal rights and obligations turn on whether the information disseminator exercised "editorial control." With control comes perks: the power to deny access and content-discriminate, the availability of copyright protection, constitutional protections such as no prior restraints, and statutory protections such as enhanced restrictions on searches and seizures, and in the case of newspapers, exemptions from antitrust provisions.

Nothing comes free, though. Entities that exercise editorial control also can be liable for defamation, obscenity, and injuries resulting from advertisements that are dangerous on their face. With minor exceptions, entities that do not exercise control, such as secondary publishers (information carriers such as bookstores) or common carriers, generally are exempt from such liability but lose some power to control content or deny access based on content.

One possible approach is obvious: control without liability. Prodigy has argued as much; even though Prodigy seeks the power to exercise editorial control, it believes it should be liable in tort only if it "endorses" its users' statements.[10]

The problem is that control without liability screws up the tort system. One of the tort system's purposes is deterrence through the accurate conveyance of social costs of actions. If Prodigy takes an action, and then does not internalize the subsequent costs, then the tort system fails to function properly.

On the other hand, sysops who do not exercise control act as information conduits and perform a valuable function in a society relying on the free flow of information. Therefore, in the only reported case to address these issues directly, *Cubby, Inc. v. CompuServe, Inc.*, the court held that CompuServe was such an important instrument in the flow of information that it would be unreasonable to hold CompuServe liable for defamation if CompuServe did not exercise editorial control.[11]

The *Cubby* approach of linking cost internalization and editorial control makes sense, but can be taken one step further: the sysop should be allowed to *choose* whether or not to exercise editorial control.[12] There are incentives to exercising editorial control, not the least of which may be economic profits,[13] but those who take on the editorial control must take the complete package, including the associated liabilities. On the other hand, those sysops who wish to be information conduits, and not exercise editorial control, are serving a valuable function in our democratic society and therefore deserve the social subsidy of tort immunity.

Despite the policy interests in unrestricted information flows, the subsidy should not be complete. To give victims some recourse, those conduits who have actual knowledge that the information they are transmitting is causing harm (i.e., defamatory remarks, obscene material) should have the duty not to transmit that material.

Allowing sysops to choose whether or not to exercise editorial control would result in a system where sysops receive different packages of rights and responsibilities based on their actions. Neither package is intrinsically detrimental to the interests of third parties; rather, both packages properly incorporate

competing policy considerations in establishing when sysops should be considered a causal agent.

Importantly, the two-tiered system could also adjust to sysops' control on a function-specific basis: sysops could exercise content control in their public message posting section but not in the private email or chat sections, or even in some but not all public message posting areas. This function-specific choice would resolve some of the nagging problems that have plagued the development of laws that purportedly apply across functions. Sysops could then exercise some control on some areas of their BBS without triggering higher level duties for the entire BBS.

Special Constitutional Considerations

Harvard Law School Professor Lawrence Tribe has said, it is "as if the Constitution had to be reinvented with the birth of each technology."[14] In their zealousness to address the problems outlined above, some state actors have bypassed constitutional procedural protections in cyberspace. While these shortcuts might reduce the harm inflicted on third parties, the Constitution has definitively enacted certain protections of civil liberties that are the price of our democracy. Therefore, despite the temptations available should we abandon these protections, we must vigilantly ensure their continued vitality in cyberspace.

Constitutional Protections Against State Intrusion.

In a famous Warren Court opinions, Justice Douglas reasoned that the Bill of Rights created certain "zones of privacy" which were off-limits from government intrusion.[15] Until recently, these zones were partially protected by the combination of physical barriers and the overwhelming volume of physical space.

These protections are lacking in cyberspace: state actors can monitor BBSs without anyone knowing; police who seize a single BBS hard drive can search every message and file on the hard drive; a key word search can find every instance of the word "cocaine." While the Electronic Communications Privacy Act[16] forbids sysops from unilaterally disclosing the contents of messages to third parties in the absence of a search warrant, a search warrant presumably could disclose information retained on backups dating to the BBS's beginning. This type of historical information is unretrievable in the case of phone calls or physical actions.

All of these dangers are compounded by the ineptitude of government actors responsible for "protecting" civil liberties in cyberspace. Even though the Steve Jackson[17] and Craig Neidorf[18] cases apparently have been resolved favorably, the chilling effect is still potent. In the sysop legal manual *SysLaw*, the authors spend almost thirty pages talking about what to do when police come to the sysop's house looking for computers.[19]

Lawrence Tribe has proposed a Twenty Seventh Amendment to the Constitution, which in essence says that all of the constitutional protections against search and seizure and other government intrusions should apply in electronic space just as they do in physical space. While stronger judicial enforcement and law enforcement restraint could lead to the same result, the point is clear: the need for reinforced procedural protections is made transcendentally important by the technology's special powers.

The Threats to Associational Privacy

As our society has evolved, associational freedom has taken on special meaning in an urban society. If I, a resident of Los Angeles, see an XXX movie in Orange County, there is a virtually zero chance that anyone would find out against my wishes: I would not have to reveal my identity, and the other theatergoers and the movie theater employees would only know me by physical description. But if I browse the pornographic GIF files on a BBS and the computer tracks my actions, the computer could later reveal how long I browsed, the files I looked at, and the files I uploaded or downloaded. If this information gets disclosed later (even years later), either voluntarily by the sysop or involuntarily through state action, I would lose my intended privacy.[20]

In a holding that could protect associational privacy, the Supreme Court held that state actors could disclose an association's membership list only if the disclosure could survive strict judicial scrutiny.[21] If future courts extend this holding naturally, all of the types of state-forced disclosure discussed above should require similarly heightened judicial scrutiny. However, this requirement still would not apply to voluntary disclosure by private party sysops, although the aggrieved user may have contractual rights or recourse such as an invasion of privacy action.

CONCLUSION

The scope of this paper indicates that we have encountered new legal frontiers, a Wild West of Laws. Until the laws "civilize" the frontier, a process that could take years given the current pace of technological development, the pioneers must act on instinct and hope. However, I have tried to show that existing laws, modified to reflect the specific facts of the new technology and properly confined in scope, can accommodate the expansion in decentralized power and lead to an appropriate balance between benefits and wrongs.

Ultimately, though, I believe the appropriate balance will be struck by the free market. So long as we create a regime where sysops internalize just social costs, the market will help sysops make appropriate choices and thereby reach one of any number of possible and beneficial market equilibria. Only if there are breakdowns in the competitive market, such as monopolization or defective cost/benefit internalization, should we reconsider the necessity of more extensive government regulation.

ENDNOTES

This paper is distilled from my article entitled *Cyberspace, the Free Market, and the Free Marketplace of Ideas: Recognizing Legal Differences in Computer Bulletin Board Functions*, scheduled for imminent publication in the Hastings Communication and Entertainment Law Journal (Volume 18, Issue 1). I thank John Brice, Michael Godwin, Esq., Sandra Goldstein Hirsh, Stuart Hauser, Carl Kadie, Anthony Klein, Esq., Gail Schlachter, Sandy Shepard, Marc Smith, Professor Tracy Westen, and Lee White, for their generosity with their time and thoughts.

[1] On-line services such as Prodigy and CompuServe provide bulletin board forums and software exchanges; hobby boards often provide information databases; and electronic networks such as the Internet provide access to on-line services such as Dialog and bulletin board and chat functions.

[2] Ithiel de Sola Pool, TECHNOLOGIES OF FREEDOM 229 (1983).

[3] *See, e.g., Lynch Predicts Sharp Correction in Stock Market*, SAN JOSE MERCURY NEWS, June 9, 1993, at 2C (John Lynch, the manager of the best performing mutual fund between 1977 and 1990, offered stock market prognostications in response to another user's query on Prodigy's Money Talk Forum).

[4] Jon Katz, *Bulletin Boards: News from Cyberspace*, ROLLING STONE, April 15, 1993, at 35.

[5] Unfortunately, many sysops use "form" contracts that appear briefly on the screen and require acceptance before the user is given access. If challenged, these contracts may be deemed "contracts of adhesion" and therefore unenforceable.

[6] The First Amendment prohibits government regulation of private associations. However, individual states may regulate associations if the regulation can survive the highest level of judicial scrutiny; therefore, Minnesota's prohibition of sexual

discrimination in places of public accommodation was upheld even as applied to a private association. *See* Roberts v. United States Jaycees, 468 U.S. 609 (1984).

Numerous constitutional provisions restrict government regulation of private property for communication purposes. *See, e.g.*, Wooley v. Maynard, 430 U.S. 705 (1977) (New Hampshire could not force state residents to place a license plate with the slogan "Live Free or Die" on their cars); Pacific Gas & Elec. Co. v. Public Util. Comm'n, 475 U.S. 1 (1986) (private groups had no right to access private gas company mailers); Hudgens v. NLRB, 424 U.S. 507 (1976) (no First Amendment right to protest at a private shopping center); Loretto v. Teleprompter Manhattan CATV Corp., 458 U.S. 419 (1982) (state law requiring apartment building owners to give physical access to cable companies was a Fifth Amendment "taking").

[7] Tcimpidis was briefly arrested after stolen telephone credit card numbers were found on his BBS, even though Tcimpidis had no knowledge that the numbers were there.

[8] *See, e.g.*, 18 U.S.C.A. § 1029 (West Supp. 1992) (making it a misdemeanor to publish computer passwords); CAL. PENAL CODE § 484j (West 1988) (prohibiting publishing computer passwords and bank account numbers on BBSs).

[9] *See, e.g.*, Robert Charles, Note, *Computer Bulletin Boards and Defamation: Who Should Be Liable? Under What Standards?*, 2 J.L. & TECH. 121 (1987).

[10] W. John Moore, *Taming Cyberspace*, 24 NAT'L J. 745, 748 (1992).

[11] Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991). CompuServe hires independent contractors as sysops for all of its forums. One of these sysops contracted with an independent on-line magazine publisher who disseminated allegedly defamatory statements. Because CompuServe did not exercise editorial control over the sysop, and certainly not over the independent magazine, the court conceptualized CompuServe's role as a library who is not responsible for the contents of all the books on the shelf.

[12] By editorial control, I do not include the ubiquitous practice of cleaning up "junk postings" to ensure that discussions stay on topic. Some, like Prodigy, prescreen; others do it after the fact, periodically or sporadically. This maintenance function is less editorial control than content "massaging." To avoid clogged channels, which create a Tower of Babel, this type of system maintenance should not be considered editorial control *so long as* the control exercised is merely redirecting misplaced postings and not other forms of control.

[13] Prodigy, positioning itself as the "Disney Channel" of BBSs, has subscribed over two million users (almost twice as many as number 2 CompuServe) in five years of existence.

[14] Don Clark, *27th Amendment Proposed for High-Tech*, S.F. CHRON., Mar. 27, 1991, at C1, C2.

[15] These zones of privacy are the "penumbras and emanations" of the First, Third, Fourth, Fifth, and Ninth Amendments. Griswold v. Connecticut, 381 U.S. 479 (1965).

[16] 18 U.S.C. §§ 2701-2703 (1988).

[17] In response to their belief that a Steve Jackson Games, Inc. employee was a hacker, Secret Service agents seized the company's computers, files, and disks. In truth, the company was writing a computer role playing game about a hacker. The plaintiffs were awarded over $50,000 under the Privacy Protection Act and Electronic Communication Privacy Act. *See* Steve Jackson Games, Inc. v. Secret Serv., 1993 WL 83042 (W.D. Tex. Mar. 12, 1993).

[18] Police arrested Craig Neidorf after Neidorf published in his magazine *Phrack* an allegedly stolen document, purportedly worth $79,449, involving the telephone emergency 911 system. After several days of trial, the prosecution dropped the charges when it realized that the document was publicly available for sale for $13. *See* 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).

[19] Lance Rosé & Jonathan Wallace, SYSLAW 127-54 (2d ed. 1992).

[20] In 1992, the Air Force initiated court martial proceedings against Col. James A. Maxwell after it learned that Maxwell had allegedly used America Online to search for restaurants that cater to homosexuals and to download homoerotic pornography. *See Colonel Faces Court-Martial After Gay Activities Alleged: Air Force Officer Blasts 'Innuendo'*, HOUSTON POST, Dec. 21, 1992, at A1.

[21] Gibson v. Florida Legislative Investigative Comm., 372 U.S. 539 (1963).

John Arnold, *The Medium is Messages*, MIAMI HERALD, Sept. 28, 1985, at 1D.

Robert Beall, Note, *Developing a Coherent Approach to the Regulation of Computer Bulletin Boards*, 7 COMPUTER/L.J. 499 (1987).

Loftus E. Becker, Jr., *The Liability of Computer Bulletin Boards for Defamation Posted by Others*, 22 CONN. L. REV. 203 (1989).

Lynn Becker, *Electronic Publishing: First Amendment Issues in the Twenty-First Century*, 13 FORDHAM URB. L.J. 801 (1985).

Philip Becker et al., INTRODUCTION TO PC COMMUNICATIONS (1992).

Judith Berck, *It's No Longer Just Techno-Hobbyists Who Meet by Modem*, N.Y. TIMES, July 19, 1992, § 3, at 12.

Charles Cangialosi, *The Electronic Underground: Computer Piracy and Electronic Bulletin Boards*, 15 RUTGERS COMPUTER & TECH. L.J. 265 (1989).

Edward A. Cavazos, Note, *Computer Bulletin Board Systems and the Right of Reply: Redefining Defamation Liability for a New Technology*, 12 REV. LITIG. 231 (1992).

Robert Charles, Note, *Computer Bulletin Boards and Defamation: Who Should Be Liable? Under What Standards?*, 2 J.L. & TECH. 121 (1987).

Edward M. Di Cato, *Operator Liability Associated with Maintaining a Computer Bulletin Board*, 4 SOFTWARE L.J. 147 (1990).

Fourth Annual Benton National Moot Court Competition: System Operator Liability for Defamatory Statements Appearing on an Electronic Bulletin Board, 19 J. MARSHALL L. REV. 1107 (1986).

Gina M. Garramone et al., *Uses of Political Bulletin Boards*, 30 J. OF BROADCASTING & ELECTRONIC MEDIA 325 (1986).

Jonathan Gilbert, Note, *Computer Bulletin Board Operator Liability for User Misuse*, 54 FORDHAM L. REV. 439 (1985).

Eric C. Jensen, Comment, *An Electronic Soapbox: Computer Bulletin Boards and the First Amendment*, 39 FED. COMM. L.J. 217 (1987).

Mitchell Kapor, *Civil Liberties in Cyberspace: When Does Hacking Turn from an Exercise of Civil Liberties into Crime?*, SCI. AM., Sept. 1991, at 158.

M. Ethan Katsh, *The First Amendment and Technological Change*, 57 GEO. WASH. L. REV. 1459 (1989).

M. Ethan Katsh, THE ELECTRONIC MEDIA AND THE TRANSFORMATION OF LAW (1989).

Jon Katz, *Bulletin Boards: News from Cyberspace*, ROLLING STONE, Apr. 15, 1993, at 35.

Peter H. Lewis, *On Electronic Bulletin Boards, What Rights Are at Stake?*, N.Y. TIMES, Dec. 23, 1990, § 3, at 8.

Jay R. McDaniel, Note, *Electronic Torts and Videotex -- At the Junction of Commerce and Communication*, 18 RUTGERS COMPUTER & TECH. L.J. 773 (1992).

Don Oldenburg, *The Law: Lost in Cyberspace*, WASH. POST, Oct. 1, 1991, at E5.

Henry H. Perritt, Jr., *Tort Liability, the First Amendment, and Equal Access to Electronic Networks*, 5 HARVARD J.L. & TECH. 65 (1992).

Andrew Pollack, *Free-Speech Issues Surround Computer Bulletin Board Use*, N.Y. TIMES, Nov. 12, 1984, at A1.

Ithiel de Sola Pool, TECHNOLOGIES OF FREEDOM (1983).

Lance Rose & Jonathan Wallace, SYSLAW (2d ed. 1992).

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 (1992).

John T. Soma et al., *Legal Analysis of Electronic Bulletin Board Activities*, 7 W. NEW ENG. L. REV. 571 (1985).

Michael L. Taviss, Comment, *Dueling Forums: The Public Forum Doctrine's Failure to Protect the Electronic Forum*, 60 U. CIN. L. REV. 757 (1992).

Lawrence H. Tribe, AMERICAN CONSTITUTIONAL LAW (2d ed. 1988).

Kim Uyehara, *Computer Bulletin Boards: Let the Operator Beware*, STUDENT LAW., Apr. 1986, at 28.