UIC John Marshall Journal of Information Technology & Privacy Law

Volume 7
Issue 4 *Computer/Law Journal - Fall 1987*

Article 3

Fall 1987

Developing a Coherent Approach to the Regulation of Computer Bulletin Boards, 7 Computer L.J. 499 (1987)

Robert Beall

NOTES

DEVELOPING A COHERENT APPROACH TO THE REGULATION OF COMPUTER BULLETIN BOARDS

I. INTRODUCTION

Personal computers have tremendously increased individuals' access to information. One of the primary mediums for exchange of information between users of personal computers is electronic Bulletin Board Systems (BBSs).[1] BBSs allow users of personal computers to network, linking their computers together through the telephone system.[2] Any personal computer owner with a telephone modem (a device which allows computers to talk to one another over the telephone lines) has access to this valuable information and communication.

BBSs are the computerized equivalent of the bulletin board at the local supermarket. A computer owner with a telephone modem and communicating software[3] has access to an estimated 3,500 to 4,500 BBSs nationwide.[4] These BBSs contain information which can be accessed and supplemented by anyone who dials the proper telephone number. Bulletin boards facilitate exchanging messages, asking questions, or posting "for sale" notices. The most popular use of BBSs is "messaging". In virtually all BBSs, a user can scan and read messages previously posted, and post messages and bulletins for other users to read.[5]

The use of BBSs involves a few simple steps. First, a user turns on his computer and, using his telephone modem, dials the correct telephone number of a computer bulletin board. When the telephone rings, it is automatically answered, and the user's computer is connected to

1. Electronic Bulletin Board Systems (BBSs) are basically files of information, stored in the memory of a computer, which are accessible through a telephone connection. For an excellent discussion of the technical advances in BBSs, see Stone, *Taking Notice of Bulletin Boards*, PC MAG., Apr. 30, 1985, at 261.

2. *See* Hoffmann, *Across the Boards*, PC MAG., June 11, 1985, at 311.

3. Crocker, *Bulletin Board Basics*, MICROCOMPUTING, Oct. 1984, at 30.

4. Soma, Smith and Sprague, *Legal Analysis of Electronic Bulletin Board Activities*, 7 W. NEW ENG. L. REV. 571, 572 (1985).

5. Crocker, *supra* note 3, at 31.

the bulletin board computer. BBSs, other than those which are commercially run,[6] are set up by a System Operator (commonly referred to as the SYSOP). The SYSOP is responsible for establishing the framework and procedures for accessing the BBS.[7] Generally, once the computers are linked, the user is greeted by an opening message supplied by the SYSOP. In most cases the user is then asked to submit his name and geographic location before proceeding.[8] After completing these formalities, the user is asked to submit, or is given, a password to access the sytem.[9] Access is relatively simple since most BBSs are designed to accommodate use by the general public.[10]

Once a caller has accessed the BBS, he can type messages which are sent, via the telephone connection, directly to the bulletin board computer where they are stored. These entries appear simultaneously on his own computer. Once the user hangs up, another caller can connect with the bulletin board computer, read the file, and add any information of his own.

There are basically three types of BBSs. First, there are hundreds of private computer bulletin boards used by businesses, schools, government agencies, and professional organizations to keep in touch with members or employees.[11]

Second, there are a small number of commercial bulletin boards which are operated for profit by large corporations. The largest of these are CompuServe, The Source, and the Dow-Jones News/Retrieval System.[12] These systems offer a wide selection of BBSs dealing with a multitude of topics. By using a telephone modem, computer operators log on to special-interest bulletin boards to exchange information on subjects ranging from Apple Computer to gardening.[13] It is even possible to carry on a simultaneous conversation with another user with CompuServe's "Citizen's Band Simulator".[14] These commercially oper-

---

6. *See infra* notes 12-15 and accompanying text.

7. For a detailed description of the process of logging on to a BBS, see McGill, *Newest City Meeting Places are in Computers*, N.Y. Times, March 21, 1984, at B1, col. 1.

8. *Id.*

9. Reid, *Computers Becoming Nation's Bulletin Board*, Wash. Post, July 19, 1985, at A4, col. 1.

10. Crocker, *supra* note 3, at 30.

11. Reid, *supra* note 9.

12. *Id.*

13. *See generally*, Lasden, *Of Bytes and Bulletin Boards*, N.Y. Times, Aug. 4, 1985, § 6 (Magazine), at 34.

14. The "CB Simulator" operates like a Citizen's Band Radio. Two users can carry on a simultaneous conversation, leaving messages on the computer screen, without hanging up the telephone and going off-line. This procedure is different from that employed with personal BBSs, where a user is generally required to go off-line in order to allow the subsequent user to access the BBS.

ated BBSs generally charge fees ranging upward from six dollars per hour.[15]

Finally, most prevalent are the free bulletin board systems which are operated around the United States by individuals primarily as a hobby. Usually, the SYSOP provides for public access, and the BBS dispenses conversation and information.[16] The subject matter on these BBSs includes such diverse topics as dating opportunities,[17] foreign policy,[18] wine tasting,[19] and parapsychology.[20] An overwhelming majority, however, facilitate communication about microcomputer software, hardware, and communications (hardware and software).[21] There are generally no fees for the use of these services, although callers have to pay any long-distance charges incurred while they are connected to the BBS.

The relative ease and low cost of setting up a BBS contribute to their growing popularity. All that is required is a personal computer, a telephone modem, and some relatively inexpensive software.[22] The entire cost of the initial set-up can be as little as $2,000.[23] The number of boards available to the millions of households capable of accessing them appears to be increasing dramatically each week.[24] Thus, the BBS represents an extremely important information service that has a tremendous potential for providing instantaneous international communication among large numbers of people who are physically removed from each other and who will probably never meet in person to discuss issues which can have a far-reaching effect.

II. OVERVIEW OF THE PROBLEM

BBSs are becoming an increasingly powerful medium of communication, but their potential has recently been overshadowed by reports of the increasing malevolent behavior of BBS users. While the vast majority of messages on BBSs involve the routine exchange of harmless information, thoughts, and chatter, law enforcement officials have become

15. Reid, *supra* note 9.

16. Reid, *supra* note 6.

17. Reid, *supra* note 9.

18. Rempel, *Abuse Hits Computer Networking*, L.A. Times, Aug. 1, 1985, § 1, col. 1.

19. For example, a BBS entitled "On-line Wine". Reid, *supra* note 9.

20. For example, a BBS in Denver is devoted entirely to users who exchange near-death experiences. Lasden, *supra* note 13, at 36.

21. Lasden, *supra* note 13, at 36.

22. Reid, *supra* note 9.

23. Reid, *supra* note 9.

24. Ralph Nader observed that the BBSs are an enormously important information resource. The relative inexpense of setting up a BBS makes them "the lowest barrier to entry of any mass communication medium". Reid, *supra* note 9.

concerned about the traffic of illegal information.[25] The FBI has investigated a child molestation ring which used BBSs to post the names and addresses of their victims.[26] Systems have also been used to exchange methods of illegally accessing corporate and government computers ("hacking").[27] Another common problem is software piracy—individuals "download" copies of software in response to BBS requests.[28] The software industry estimates that the majority of its $1.5 billion of sales lost to piracy can be attributed to computer bulletin boards.[29]

This Note focuses primarily upon the use of BBSs by "phreakers"—individuals who specialize in making telephone calls without paying, primarily by obtaining telephone credit card numbers and posting them on BBSs. This problem is inherent in the use of BBSs, since networking requires the use of telephone lines, and often lengthy long-distance calls to use a distant bulletin board. Further, many BBS users are minors.[30] They often lack adequate resources to pay telephone charges, and would rather escape payment by the unauthorized use of credit card numbers than suffer the wrath of their parents when the household telephone bill arrives.

In response, telephone companies have become increasingly interested in monitoring and reporting BBSs with credit card numbers posted on them to the authorities.[31] The telephone companies believe that a substantial percentage of the losses resulting from the unauthorized use of credit card numbers can be attributed to the BBSs, because a credit card number which is posted on a BBS becomes readily available to all of the system's users.[32] As a result of these efforts by the telephone companies to thwart the distribution of such credit card numbers, the SYSOPs operating these "phreaker" BBSs have become more sophisticated. Consequentially, the boards have become more difficult to investigate.[33]

If the SYSOP openly encourages and permits messages containing stolen credit card numbers to be posted on his BBS, the authorities

25. For an excellent discussion of the growing concern over the misuse of BBSs, see Soma, *supra* note 4, at 572-74.

26. Lasden, *supra* note 13, at 40.

27. Landreth, *Inside the Inner Circle*, POPULAR COMPUTING, May 1985, at 62. *See also* Lery, *Bummed to the Minimum, Hacked to the Max*, ACCESS (Speical Issue NEWSWEEK), Fall 1984, at 1011.

28. Lasden, *supra* note 13, at 42.

29. Lasden, *supra* note 13, at 42.

30. Soma, *supra* note 4, at 576.

31. Rempel, *supra* note 18, at 16.

32. Pacific Bell reports that stolen credit card numbers are costing U.S. telephone companies one hundred million dollars. Pemberton, *Information Mischief?. . .Information Villainy?—The Tcimpidis Case*, DATABASE, Feb. 1985, at 6.

33. Rempel, *supra* note 18, at 16.

have legal authority to shut down the bulletin board. This Note, however, focuses on the liability of a legitimate BBS SYSOP when stolen credit card numbers are posted on his system by someone else. Most SYSOPs agree that most BBSs have carried illegal information at some time.[34] Resolving the issue of SYSOP liability, therefore, is tremendously important.

These issues were brought to the forefront by a much publicized incident involving Tom Tcimpidis. Tcimpidis was a SYSOP who maintained a BBS named MOG-UR which was intended to facilitate the exchange of information pertaining to system software, trade tips, and other technical data.[35] Among approximately one thousand legitimate messages, Pacific Bell security officers allegedly found one Pacific Bell credit card number and two Sprint access codes posted on the message area of MOG-UR.[36] The Los Angeles Police, acting on this information and armed with a search warrant, seized Tcimpidis' computer equipment.[37] Tcimpidis was charged with "knowingly and willfully publishing" the numbers with the intent that they be used to avoid telephone charges.[38] The charges filed against Tcimpidis were ultimately dismissed. This case was the first of its kind, however, and succeeded in raising important questions regarding the potential criminal liability of SYSOPs for messages posted on their BBSs.

This Note focuses on the SYSOP's potential liability for messages pertaining to the illegal use of telephone services. This problem is not only widespread in the BBS community, but constitutes the single greatest potential threat of liability for a SYSOP.

III. EXISTING LAW

A. STATE TELECOMMUNICATIONS STATUTES

All states have some sort of statutory provision dealing with the theft of telecommunications. An examination of current law, however, reveals its inability to deal effectively with the types of problems presented in the Tcimpidis case.

Every state has either a theft of telecommunications statute or a theft of service statute which includes telecommunications.[39] These statutes focus on the actual fraudulent "use" of the telecommunications

34. Watt, *Police Raid Worries SYSOPs*, INFOWORLD, July 9, 1984, at 30-31.

35. *Id.* at 30. *See also*, Stipp, *Computer Bulletin Boards Fret Over Liability for Stolen Data*, Wall St. J., Nov. 9, 1984, at 33, col. 1 (discussing the facts of the Tcimpidis case).

36. *Id.*

37. *Id.*

38. *Id.*

39. For a detailed description of state law provisions dealing with computer crime, see Soma, *supra* note 4, at 577-603.

service—the actual use of a stolen credit card number to obtain telephone services.[40] In cases where the credit card number is merely posted on a BBS, however, the SYSOP does not actually use the code number to obtain telephone services. These statutes do not become applicable, therefore, until an individual actually uses the credit card number posted on the BBS to fraudulently obtain these services. The SYSOP who operates a board which posts stolen credit card numbers is beyond the reach of these laws unless he actually uses the information himself.

The theft of telecommunication by "device" statutes are also inapplicable to the activity of the SYSOP.[41] These statutes generally prohibit the use, possession, or sale of such a device, as well as plans and specifications to build the device.[42] They deal with the use of equipment such as "blue boxes".[43] These provisions apply to the use or actual possession of the device and the activity of the "phreaker"—not to the SYSOP whose BBS contains information relating to such activity.

A third type of state statute which attempts to deal with these "phreaker" activities prohibits the publication of telephone credit card codes and plans for telecommunications theft devices.[44] This is precisely the type of statute under which charges were filed against Tcimpidis.[45] The key issue in applying this type of statute to SYSOPs is the meaning of "publication". The California Penal Code defines "publication" as the "communication of information to any one or more persons, either orally, in person or by telephone, radio or television, or in a writing of any kind, including. . .a letter or memorandum, circular or handbill, newspaper or magazine article, or book."[46] Undoubtedly, this statute would apply to the user of a BBS who posted a stolen credit card number or to a SYSOP who actively encouraged the posting of this subject matter. A more important, yet unresolved, issue is whether or not these types of statutes apply to the SYSOP of a legitimate BBS (*i.e.*, one dedicated to the discussion of legal subject matter) when illegal information is posted on his board.

The definition of "publication" under section 502.7(c) appears to be

---

40. *See, e.g.*, CAL. PENAL CODE § 502.7 (West Supp. 1984), which pertains to obtaining telephone service by fraud, including the obtaining of telephone services with intent to defraud, by unauthorized use of a telephone credit code, trick, or device.

41. *See, e.g.*, CAL. PENAL CODE § 502.7(b) (West Supp. 1984).

42. *Id.*

43. A "Blue Box" is a device which is capable of imitating telecommunications tones and is used to make toll free long-distance calls. *See* Rosenbaum, *Secrets of the Little Blue Box*, ESQUIRE, Oct. 1971, at 116.

44. *See, e.g.*, CAL. PENAL CODE § 502.7(c) (West Supp. 1984).

45. Watt, *supra* note 34, at 31.

46. CAL. PENAL CODE § 502.7(c) (West Supp. 1984).

premised upon some affirmative act by the would-be publisher. It may be argued that because the posting of the message on the SYSOP's board involves no affirmative action on his part, other than the initial set-up of the BBS, a SYSOP's actions do not constitute publishing, and thus the statute does not apply.[47]

In addition, even if a court finds that the SYSOP's role constituted publishing, the prosecuter must prove that the publication was made "with knowledge or reason to believe that it [would] be used to avoid the payment of a lawful charge."[48] It would probably be necessary to prove, therefore, that the SYSOP was at least aware of the message on his board. The sheer volume of messages on any single BBS suggests that no single SYSOP could be aware of everything posted on his board, including the stolen credit card number. Thus, if the number was published without his knowledge, there would be no finding of the requisite intent.

Although this type of statute has been used effectively against traditional forms of publication, such as newspapers,[49] and has withstood constitutional challenges,[50] the dynamics of this new computer technology provide added difficulties. Of particular importance is the evidentiary problem, noted by commentators, of "shoe-horning" the new technology into the current framework of the law.[51]

B. FEDERAL STATUTES

Federal law has not yet been developed to handle the problems associated with the new technology of computer BBSs. The computer prosecutions which have taken place under federal law have come primarily under the Wire Fraud Act.[52] The Wire Fraud Act is extremely broad, giving the government the authority to prosecute:

> [w]hoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or

47. Proponents of this argument often compare the BBS to a public bulletin board at a grocery store—if someone posted illegal messages such as solicitation for prostitution, credit card numbers, or telephone codes, would the cops shut down the stores? Watt, *supra* note 34, at 31.

48. CAL. PENAL CODE § 502.7(c) (West Supp. 1984).

49. *See* State v. Northwest Passage, Inc., 17 Wash. App. 658, 564 P.2d 1188 (1977), *rev'd*, 90 Wash. 2d 741, 585 P.2d 794 (1978), which involved the newspaper publication, in violation of a state statute, of information pertaining to AT&T's method of establishing telephone credit card code numbers.

50. *Id.* The Washington Supreme Court held that the statute did not substantially restrict protected speech when judged in relation to the statute's legitimate function of preventing fraud. 90 Wash. 2d at 746, 585 P.2d at 796.

51. *See generally*, Comment, *Computer Crime—Senate Bill S.240*, 10 MEM. ST. U.L. REV. 660, 661-62 (1980).

52. 18 U.S.C. § 1343 (1982).

> fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio or television communication in interstate or foreign commerce, any writings, signs, signals, pictures or sounds for the purpose of executing such a scheme or artifice.[53]

Although this statute appears to be quite broad, the majority of the prosecutions relating to computer crime under its provisions have dealt with problems of unauthorized access or "hacking".[54] Even if the government were to use this statute to deal with the "phreaking" activity on BBSs, it would face the problems inherent in applying the traditional penal laws to new technology.[55]

The only other significiant piece of federal legislation dealing with computer technology is the "Counterfeit Access Device and Computer Fraud and Abuse Act of 1984."[56] This statute is inapplicable to the problems associated with "phreaker" activity on BBSs because it deals exclusively with the problem of unauthorized access.[57]

Thus, there is currently no effective law, state or federal, to deal with the issues raised in the Tcimpidis case. Given the fact that most observers, including the SYSOPs,[58] believe that these are serious problems that warrant attention, this Note will attempt to devise a satisfactory scheme of regulation for all interests involved.

IV. MODELS OF REGULATION[59]

Current state and federal law is not able to deal effectively with the issues raised in the Tcimpidis case. In order to develop an effective means of regulation, one must first look to traditional regulatory schemes for newspaper publishers and common carriers. The question of responsibililty for criminal, libelous, or obscene information has an answer which depends upon whether BBS "publication" is governed by the laws pertaining to newspapers or those pertaining to common carriers.

---

53. *Id.*

54. *See* United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978), *cert. denied*, 441 U.S. 922 (1979) (involving the unauthorized access of a computer to obtain software stored within the accessed computer).

55. For a comprehensive list of cases which address this difficulty, see Becher, *Electronic Publishing: First Amendment Issues in the Twenty-First Century*, 13 FORDHAM URB. L. REV. 801, 802 n.7 (1985).

56. Pub. L. No. 98-473, 1984 U.S. CODE CONG. & ADMIN. NEWS. (98 Stat.) 2190 (to be codified at 118 U.S.C. § 1030).

57. *Id.*

58. *See generally* Stipp, *supra* note 35, at 33, col. 1.

59. *See generally* Becher, *supra* note 55, at 828-58 (discussing the regulation of both the press and common carriers in detail and also providing a discussion of the regulation of the broadcast medium).

A. THE REGULATION OF THE PRESS

BBSs are similar to newspapers in that they are responsible for the distribution of printed information through messaging and on-line information services. The press has traditionally been afforded protection from government interference in order to facilitate unrestrained debate on matters of public interest. Government interference with the editorial decisions of newspapers regarding content and the characterization of public issues is not consistent with the rights afforded by the First Amendment.[60] Nonetheless, the Supreme Court has recognized that some government interference is permissible when the content of the speech is deemed "obscene" or "defamatory".

1. *Obscenity*

The Supreme Court, in *Roth v. United States*,[61] stated that speech deemed "obscene" is "utterly without redeeming social importance" and, therefore, is not entitled to the protections afforded by the First Amendment.[62] The Court established that whether or not material is "obscene", and thereby excluded from protection under the Constitution, depends upon whether the dominant theme of the material appeals to the prurient interest of an average person applying contemporary community standards.[63]

The Court offered a clearer test for "obscenity" in *Miller v. California*.[64] The "Miller Test" utilizes the following three elements to determine whether or not material is legally "obscene":

> (a) whether the average person applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political or scientific value.[65]

If there is an affirmative answer to all three of these questions, then the material is deemed legally "obscene", and the government is entitled to ban the material from being published and distributed.

2. *Defamation*

Defamation is the other significant constraint on the First Amendment guarantee of freedom of the press. The Court has similarly cho-

60. Miami Herald Publishing Co. v. Tornillo, 418 U.S. 241, 258 (1974).
61. 354 U.S. 476 (1957).
62. *Id.* at 484.
63. *Id.* at 489.
64. 413 U.S. 15 (1973).
65. *Id.* at 24 (citations omitted).

sen to exclude "defamatory" material from First Amendment protection in order to protect the interest of personal reputation.[66]

Originally, defamatory publications received no First Amendment protection, and truth was the only affirmative defense in a defamation suit. In *New York Times Co. v. Sullivan*,[67] however, the Court articulated a standard for determining when a media defendant, such as the printed press, may be held liable for defamatory publications. In this landmark decision, the Court created a privilege whereby media defendants were liable for defamatory publications concerning public officials only when the statements were made with "actual malice."[68] Thus, such statements are privileged absent a showing of "malice", defined as "knowledge or reckless disregard for the truth."[69] The Court established this privilege in order to prevent a "chilling effect" on the dissemination of information by the media. The rationale is that the media will be reluctant to publish any controversial material about a public official if truth is the only defense to a defamation suit.[70]

Another significant aspect of regulation based upon the defamatory content of speech is the distinction that the common law draws between defamation actions against the "primary publisher" and actions against the "secondary publisher".[71] The primary publishers, those who "print and sell newspapers, magazines, journals and the like", could be held liable for the publication of defamatory material "because they have the opportunity to know the content of the material being published and should therefore be subject to the same liability rules as are the author and the originator of the material."[72] By contrast, the secondary publishers, which include libraries, news vendors, distributors, and carriers, could not be held liable for defamatory material unless the plaintiff could establish that they changed the communication and knew or had reason to know of the defamatory nature of the statement.[73]

This distinction is justified because secondary publishers usually are unaware of the defamatory nature of the message and are not in a position to prevent or lessen the harm.[74] Thus, the degree of responsibility is fixed by the amount of discretion the publisher exercised in de-

66. Rainer's Dairies v. Raritan Valley Farms, Inc., 117 A.2d 889, 991 (1955) (defamation law many conflict with policy favoring free speech and press).

67. 376 U.S. 254 (1964).

68. *Id.* at 279-80.

69. *Id.*

70. *Id.* at 279.

71. *See* W. PROSSER & W. KEETON, PROSSER AND KEETON ON TORTS § 113, at 810-11 (5th ed. 1984).

72. *Id.*

73. *Id.*

74. Thornton, Gerlach & Gibson, *Libel in Videotex Symposium*, 36 FED. COM. L.J. 178, 179 (1984).

cisions regarding the publication of the material. With more discretion regarding publication of the material, comes a higher degree of responsibility on the part of the publisher.[75]

B. Regulation of Common Carriers

The common carrier regulatory scheme offers an alternative which is quite different from the regulation of the press.[76] Just as the BBS shares characteristics with the press medium, it also possesses a number of attributes similar to those of the common carriers. Most notable of these is the transmission of information over telephone lines.

In *National Association of Regulatory Utility Commissioners v. FCC*,[77] the Supreme Court defined a common carrier as:

> an individual or organization that holds itself out as available to the public for hire, that provides facilities thereby to all members of the public who choose to use its services to transmit information of their own design and that serves all members of the public indifferently, basing all decisions on non-discriminatory factors.[78]

Most importantly, the common carrier's responsibility is to provide a "pipeline" to facilitate the flow of communication.[79] As a result, carriers are immune from liability for message content, libel, and slander.[80]

The degree of responsibility for a common carrier is fundamentally different from that of the newspaper publisher, who is expected to oversee transmission content and may be held responsible for the material contained in the transmission. Thus, if BBSs were regulated in the same fashion as common carriers, the SYSOP could not be held responsible for the messages posted by users on the BBS.

V. REGULATION OF BULLETIN BOARD SYSTEMS

At this time, there is no coherent body of regulation concerning BBSs. One must decide by analogy, therefore, whether they should be

---

75. *Id.* at 180.

76. *See generally* Becher, *supra* note 55, at 853-58 (providing a detailed description of the "Common Carrier" model of regulation).

77. 525 F.2d 630 (D.C. Cir. 1976), *cert. denied*, 425 U.S. 992 (1976).

78. *Id.* at 640.

79. *Amendments of Parts 1, 2, 21 and 43 of the Commission's Rules and Regulations to Provide for Licensing and Regulation of Common Carrier Radio Stations in the Multipoint Distribution Service (Report and Order)*, 45 F.C.C. 2d 616, 618 (1974) [hereinafter *Report and Order*].

80. *See* Farmers Union v. WDAY, 36 U.S. 525 (1959) (broadcaster immune from defamation action when acting merely as a conduit for political messages); Edwards v. Nat'l Audubon Soc'y, Inc., 556 F.2d 113 (2d Cir. 1977), *cert. denied*, 434 U.S. 1002 (1977) (immunity of newspaper when acting as conduit for communication of reported accusation by speaker).

regulated by the laws covering newspapers[81] or by the laws covering telephone service.[82] If BBSs are considered to be merely conduits through which information flows, like a telephone service, a SYSOP, arguably, cannot be held responsible for the content of the messages posted by users of the service. If, on the other hand, the BBS is considered to be a publication, the SYSOP would be responsible for everything it publishes, including the text that appears on the screen.

Many commentators have argued that the resolution of this ambiguity lies in the Supreme Court's treatment of the *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.* case.[83] Dun & Bradstreet publishes and distributes data on the creditworthiness of companies to its subscribers. This data is usually in electronic form. Dun & Bradstreet was sued for libel by a Vermont company, Greenmoss Builders Inc., after it erroneously reported that Greenmoss had filed for bankruptcy. One of the questions facing the Court was whether the same First Amendment protection against libel for newspapers should be extended to companies like Dun & Bradstreet. The Court rejected Dun & Bradstreet's request for such protection by distinguishing between publications which disseminate news for public consumption and those which provide specialized information to a selected audience.[84] The Court, therefore, affirmed the lower court decision to allow recovery of damages against Dun & Bradstreet, absent a showing of actual malice.

While the Supreme Court's decision not to extend First Amendment protection to commercial distributors of information may have some effect on the commercially run BBSs, such as CompuServe and The Source,[85] the decision is not likely to influence the protection of non-profit, privately run BBSs. The Court's holding in *Dun & Bradstreet* was premised on the fact that the credit report was made available to only five subscribers, who, under the subscription agreement, could not disseminate it further. Thus, it could not be said that the report involved any strong interest in the free flow of commercial information.[86] In addition, the speech in this case, like advertising, was solely motivated by profit. The Court found, therefore, that the speech was unlikely to be deterred by the chilling effect of any incidental state regulation.[87] The market provides a powerful incentive for a credit reporting agency to be accurate, because a false report is of no use to creditors.

---

81. *See supra* notes 59-75 and accompanying text.
82. *See supra* notes 76-80 and accompanying text.
83. 472 U.S. 749 (1985).
84. *Id.* at 762.
85. *See supra* notes 12-15 and accompanying text.
86. 472 U.S. at 762.
87. *Id.*

Lacking these characteristics, the BBS run by a private individual is, by implication, entitled to a greater degree of First Amendment protection than a credit reporting agency. The only similarity between a privately run BBS and the credit reporting industry is the electronic distribution of information. The Court's disposition of the issues in *Dun & Bradstreet* does little to resolve the ambiguity involved with the regulation of privately run non-profit BBSs.

It may be argued that the SYSOP running a BBS should be afforded not only the protection of a newspaper publisher, but the complete immunity from liability of a common carrier. In the case of privately owned, public access BBSs, which are run as a hobby rather than for commerical incentive,[88] any liability scheme which held the SYSOP responsible for defamatory information posted on his BBS would create a "chilling effect" on the operation of such BBSs. A SYSOP is not able to research every bit of information posted on his BBS and would tend to cease operating the BBS completely, rather than face the possibility of legal action. In fact, most SYSOPs believe it would be impossible for them to operate their boards if they had to monitor all of the messages at regular intervals.[89] This rationale underlies the Supreme Court's decision in *New York Times Co. v. Sullivan*,[90] which creates a privilege for media defendants faced with defamation lawsuits.

While this decision would protect the SYSOP in a defamation action, absent a showing of actual malice,[91] the newspaper scheme of regulation would provide only limited protection when criminal information is published on the BBS.[92] If the SYSOP was considered to be a publisher, he would still be liable for the publication of stolen credit card numbers, posted by BBS users, under many state criminal statutes.[93]

Regulation similar to that imposed on common carriers would not impose any liability on a SYSOP for information posted on his BBS. The primary distinction between a common carrier and a publisher relates to the amount of editorial control exercised by each. The publisher selects the material which will go into his publication and be

88. The majority of privately owned BBSs are run primarily as a hobby. *See supra* notes 16-21 and accompanying text.

89. Pollach, *Free-Speech Issues Surround Computer Bulletin Board Use*, N.Y. Times, Nov. 12, 1984, at A1, col. 1.

90. *See supra* notes 67-70 and accompanying text.

91. Under the current law this privilege may only be asserted against the defamation claims of "public officials".

92. *See, e.g.*, State v. Northwest Passage, Inc., 17 Wash. App. 658, 564 P.2d 1188 (1977), *rev'd*, 90 Wash. 2d 741, 585 P.2d 794 (1978).

93. *Id.*

distributed. A common carrier merely supplies the means of distribution, or pipeline, through which the information flows.[94]

The rationale behind this distinction can be traced to the common law distinction between a "primary" and a "secondary" publisher.[95] As noted earlier, primary publishers are held to a higher degree of responsiblity for what they publish. Publication for a primary publisher includes gathering and writing, as well as dissemination.[96] The secondary publisher, on the other hand, cannot be held liable unless it changes the material and is negligent in failing to realize its defamatory nature.[97] Because secondary publishers are associated solely with distribution, not content, they are usually unaware of the defamatory nature of the message and are not in a position to prevent the harm.[98]

Thus, like the common carrier, the secondary publisher has very little discretion regarding the choice of the material to be transmitted. Both of these entities are involved solely in the distribution of information. The lower degree of responsibility attached to these entities reflects their limited association with the content of the material which is actually published or transmitted.[99]

Although the electronic messages on a BBS are distributed in printed form, much like a newpaper, the SYSOP's role in the distribution seems closer to that of the secondary publisher or the common carrier. The SYSOP invests his time and money to set up a BBS. These systems are intended for public access, however, and allow individuals to communicate with one another, often anonymously.[100] Although a SYSOP may provide a list of different subject matters which compose the BBS (a "menu"), he does not participate in the exchange of information between users of the BBS. In fact, he probably does not know who the users actually are, because most users use code names to sign-off on messages.[101] Most SYSOPs are overwhelmed by the sheer volume of messages posted on their system, and feel that monitoring their BBSs would be analogous to a library insuring the accuracy of each and every one of its books.

The strongest argument for releasing the SYSOP from all liability

94. *Report and Order, supra* note 79, at 618.

95. *See supra* notes 71-75 and accompanying text.

96. *Id.*

97. *Id.*

98. *Id.*

99. *Id.*

100. Most BBS users do not use their real names, but instead use "passwords" which they choose for themselves. In the vast majority of BBSs, there is no way to determine who the user actually is. However, BBSs can be set up requiring the user to leave his name and telephone number, which the SYSOP will subsequently verify, before he will be issued a password that will enable him to log-on. Watt, *supra* note 34, at 31.

101. *Id.*

for messages posted on his BBS is supplied by a line of cases which refuse to hold newspaper publishers liable when they function solely as providers of a communication pipeline. The Second Circuit, in *Edwards v. National Audubon Society, Inc.*,[102] created a constitutional privilege for the press, when it acts as a conduit by republishing defamatory comments while reporting on newsworthy events. Federal courts, applying federal law, are generally reluctant to hold the press responsible for publication of defamatory statements originally uttered by others.[103]

Under both the newspaper and common carrier regulatory schemes, the courts seldom hold the publisher/transmitter responsible when he acts merely as a conduit. In most cases, SYSOPs provide a similar service in that their BBSs provide a conduit through which users exchange information. The popularity of the BBSs, which generates a tremendous number of users, has forced the SYSOPs to assume a passive role regarding incoming messages.[104] Thus, given the current regulatory scheme for newspaper publishers and telephone companies and the judicial trend in applying these regulatory laws, a SYSOP probably would not be held responsible for the content of information posted on his BBS.

VI. PROPOSED MODEL LEGISLATION

An analysis of current regulatory schemes and judicial decisions indicates that SYSOPs of BBSs would not be legally responsible for information posted on their BBS. This conclusion is unsatisfactory, however, given the legitimate societal interest involved — preventing persons from defrauding the telephone company through use of false credit card numbers. The losses suffered from this phreaker activity must ultimately be made up by the ratepayers. Because this interest is substantial, a system must be implemented which will adequately balance the interest of the BBS community in facilitating the unrestricted flow of information among the millions of BBS users and the interest in protecting the rights of those who would be injured by information misdeeds. As a solution to this problem, this Note proposes a federal law requiring the licensing of all BBSs through the FCC.

The system must be implemented on the federal level because of the basic nature of the BBS network system. A state law would have limited application and would only encourage the creation of BBSs in

102. 556 F.2d 113 (2d Cir. 1977), *cert. denied*, 434 U.S. 1002 (1977) (immunity of newspaper from defamation liability when acting merely as a conduit for communication of reported accusation speaker).

103. *Id. See also* Farmers Union v. WDAY, 36 U.S. 525 (1959) (immunity of broadcaster from defamation when acting merely as a conduit for required political messages).

104. *See generally* Pollach, *supra* note 89.

states without regulations. The BBSs would still be accessible to users in the regulated state. Thus, the BBSs must be dealt with uniformly under the federal law.

Under the proposed system, all BBS SYSOPs would be required to submit license applications to the FCC. This is the same procedure required of applicants for amateur radio operator licenses.[105] The required information would include the operator's name, address, telephone number, and additional standard background information, as well as the access telephone number and any other information relating to information access on the BBS. Upon receipt of this application, the FCC could then issue the SYSOP a license to operate his BBS.

Opponents of this system may argue that an individual has a First Amendment right to set up a BBS and that this licensing scheme serves as an unconstitutional prior restraint on publication.[106] Although there is a strong presumption of unconstitutionality regarding prior restraints,[107] the Supreme Court has upheld such systems when specific procedural safeguards have been implemented.[108] For example, the Supreme Court recognized the competing interests of the police, in preserving public peace, and the individual, in freedom of expression, when it upheld a permit system employed to accommodate the exercise of assembly. The conditions attached to the acquisition of the permit dealt only with preserving public peace.[109] The major doctrine governing the form of permit systems is related to rules against vagueness and overbreadth.[110] The standards determining whether a permit is to be granted or denied must be sufficiently detailed so that the officials administering the system are not given unbridled discretion.[111]

In the case of BBSs, there are clearly two competing interests: (1) keeping the BBSs operating to facilitate the exchange of ideas between users, and (2) protecting the rights of others, such as the tele-

105. 47 U.S.C. §§ 303-310 (Supp. 1986).

106. A primary purpose of the First Amendment was to forbid any system of prior restraints, such as the English licensing scheme, by which nothing could be published without government or church approval. This aim remains a vital part of modern First Amendment doctrine, so that any governmental action which prevents expression from occurring is presumed to be constitutionally invalid. L. TRIBE, AMERICAN CONSTITUTIONAL LAW, at 724-26 (1978).

107. *Id.*

108. *See* Freedman v. Maryland, 380 U.S. 51 (1965).

109. Cox v. New Hampshire, 312 U.S. 569, 576 (1941).

110. A statute is "overbroad" if, in addition to proscribing activities which may constitutionally be forbidden, it also covers speech or conduct which is protected by the guarantees of free speech or free association. L. TRIBE, *supra* note 106, at 1022.

111. *See* Lovell v. City of Griffin, 303 U.S. 444 (1938) (ordinance held unconstitutional because it gave a censor's power to the City Manager and did not preserve a legitimate state interest).

phone company, who could be harmed by information misdeeds. The proposed licensing system is an attempt to protect both of these interests. Further, the proposed scheme does not create any overbreadth problems, because the FCC would be required to issue a license to all applicants who submit the required information. Thus, the discretion of the administering officials would be sufficiently limited.

The goal of this proposed licensing scheme is to have sufficient information to access all of the BBSs that are currently operated. The legislation would make failure to obtain a license for operating a BBS a misdeameanor, punishable by a fine and/or imprisonment.

In addition, the continued possession and renewal of a license to operate a BBS would be predicated upon adherence to certain rules and regulations. Primarily, the SYSOP would be required to make a good faith effort to keep his board free from information which would cause harm to others, including credit card numbers, access numbers to private computers (especially business and government computers), and bank account numbers. Publishing this information would result in notification that the information was posted on the computer and a request that it be removed. When repeated violations or lack of good faith are involved, the SYSOP's license could be revoked.[112]

Opponents may argue that budget constraints of administrative agencies, including the FCC, make the cost of monitoring BBSs for violations prohibitive. This argument assumes that the FCC would be responsible for monitoring the BBSs. The proposed system, however, would burden the FCC with the duties of maintaining the licensing information and issuing the licenses only. The duty of monitoring would fall upon the private sector, whose interests provide an incentive to monitor. This group would then report violations to the FCC for follow-up investigation. Many large corporations, notably TRW and MCI, have already undertaken such monitoring efforts.[113] In fact, MCI believes that its enforcement was initially successful, and that only more restrictive access procedures, implemented by SYSOPs, have curbed continued effective regulation. Given the willingness of these corporations to monitor the BBSs, provided they have access, this proposed licensing scheme would be an extremely efficient means of regulation.

---

112. Although "good faith" might appear to be a vague standard, there are some basic steps that could be taken by any SYSOP confronted with illegal messages on his BBS. For example, once the problem has been pointed out to the SYSOP, he could take steps to either restrict usage to individuals who have submitted a valid name and telephone number, or he could use a delay mechanism to facilitate the review of his messages. *See supra* note 100 and accompanying text for a more detailed explanation. If a SYSOP were notified of the existence of illegal messages on his board, the implementation of any of these basic measures would be considered a good faith effort.

113. *See generally* Rempel, *supra* note 18.

The information submitted to the FCC would allow anyone to monitor BBSs, which are usually meant for public access in the first place.

VII. CONCLUSION

The advent of the computer bulletin board technology demands a reexamination of the traditional models of regulation. Although the BBS shares characteristics with both the press and the common carrier, it does not appear that either of the traditional models offer an entirely statisfactory method for regulating BBSs. Regulation of BBSs as newspapers would ignore the passive role of the SYSOP in the publication of messages. The common carrier approach would neglect the interests of society in curbing the illegal messages.

This Note proposes recognition of the interests of both the individual SYSOP and of society. The proposed licensing scheme attempts to curb the posting of illegal messages by anonymous users, while imposing a minimum burden on the SYSOP. The system provides the information necessary to give the phone companies an incentive to monitor the BBSs for illegal messages. Thus, the BBSs may be monitored at a minimum cost to society and with a minimum of interference with the SYSOP.

Robert Beall