UIC John Marshall Journal of Information Technology & Privacy Law

Volume 12
Issue 2 *Computer/Law Journal - Winter 1993*

Article 1

Winter 1993

E-Law: Legal Issues Affecting Computer Information Systems and System Operator Liability, 12 Computer L.J. 101 (1993)

David Loundy

E-LAW: LEGAL ISSUES AFFECTING COMPUTER INFORMATION SYSTEMS AND SYSTEM OPERATOR LIABILITY*

by DAVID LOUNDY†

† J.D., University of Iowa Law School; B.A. Telecommunications, Purdue University. He has been active in the use and administration of computer bulletin board systems for a number of years, and serves on the Law School Computer Committee.

I. INTRODUCTION

> Over the last 50 years, the people of the developed world have begun to cross into a landscape unlike any which humanity has experienced before. It is a region without physical shape or form. It exists, like a standing wave, in the vast web of our electronic communication systems. It consists of electron states, microwaves, magnetic fields, light pulses and thought itself. It is familiar to most people as the "place" in which a long-distance telephone conversation takes place. But it is also the repository for all digital or electronic transferred information, and, as such, it is the venue for most of what is now commerce, industry, and broad-scale human interaction. William Gibson called this platonic realm "Cyberspace," a name which has some currency among its present inhabitants. Whatever it is eventually called, it is the homeland of the Information Age, the place where the future is destined to dwell.[1]

Computer information systems, as the term is used in this article, refers to a variety of computer services that, together, make up "Cyberspace." *Cyberspace* is the realm of digital data. Its shores and rivers are the computer memories and telephone networks that connect computers all over the world. Cyberspace is a hidden universe behind the automatic teller machines, telephones, and Westlaw terminals which many of us take for granted. It is also a way for computer users all over the world to interact with each other instantaneously.

At ever-increasing rates, people are beginning to see the advantages of this new electronic medium and incorporate travels into Cyberspace as

1. M. Kapor & J. Barlow, Across the Electronic Frontier, July 10, 1990 (Electronic Frontier Foundation, available over the Internet by anonymous FTP from FTP.EFF.ORG).

a regular part of their lives. However, the growth of electronic communication and data manipulation has not been matched by an equal growth in understanding on the part of legislatures, the judiciary, or the bar.

This article examines the current regulatory structure governing a few of the "Empires of Cyberspace," such as Bulletin Board Systems, electronic databases, file servers, networks, and the like. Different legal analogies that may apply will be illustrated, and some of their strengths, weaknesses, and alternatives will be analyzed. The article begins by looking at different types of computer information systems, and the major legal issues surrounding computer information systems will be surveyed in brief.[2] Next, the different legal analogies which could be applied to computer information systems will be examined. These different analogies provide an understanding of how courts have seen various communication technologies, and how more traditional technologies are similar to computer information systems. Liability for improper activities both defining what is improper and who can be held responsible has been determined by which analogy the courts apply. Finally, an evaluation will be made of where the law affecting computer information systems now stands, and how it should be developed.

A. Computer Information Systems Defined

1. *Bulletin Board Systems*

Often referred to simply as a BBS, a computer bulletin board system is the computerized equivalent to the bulletin boards commonly found in the workplace, schools, and the home. Instead of hanging on a wall covered with notes pinned up with thumbtacks, computer bulletin boards exist inside the memory of a computer system.[3] Rather than walking up to a bulletin board and reading notes other people have left or sticking up notes of his or her own, the BBS user connects his or her personal computer to the "host" computer,[4] usually via a telephone line.[5] Once

2. Each of the legal issues could be discussed in articles at least this large, so only the most important aspects will be covered.

3. To run a computer bulletin board system, three things are needed. The first item is a computer. Bulletin board systems can be run on virtually any size computer, from a small personal computer costing a few hundred dollars, to a large mainframe computer affordable only to large corporations and universities. Second, bulletin board software is needed, which can be obtained either commercially or for free. Finally, there must be a way for people (usually called "users" in computer jargon) to access the bulletin board. This is accomplished via a modem or connection to a computer network.

4. A *host computer* is the computer on which the bulletin board software runs and which stores the messages left by users of the BBS.

5. Connection via a telephone line may be accomplished by a *modem*, a device which converts computer data to an audio signal which can then be transferred over a standard telephone wire where it is received by another computer also equipped with a modem, which then converts the signal back into a form comprehensible to the receiving computer.

connected to the host computer, a user can read the notes (also referred to as messages or posts) of other users, or type in his or her own messages to be read by other users. These Computer Bulletin Boards are referred to as *systems* because they often provide additional services or several separate "areas" for messages related to different topics.[6]

Bulletin board systems can be classified in a number of ways. One way to classify them is by the number of users BBSs support simultaneously. The majority of BBSs run by hobbyists are single-user boards—they can only be used by one person at a time.[7] But some bulletin boards are able to support many users, often upwards of fifty users at once. Another way to differentiate between BBSs is by means of access: some are available only by direct dial, other BBSs are available through a network.[8]

There are a number of different things that Bulletin Board Systems users can do. As the name implies, the primary function of a BBS is as a place to post messages and read messages posted by others. Whatever the user's interests, there is probably a BBS to cater to it. However, like any communications forum, this can raise some serious First Amendment concerns over some of the potential uses, such as the posting of pornographic material, defamation, etc.

Increasingly, computers may be found connected together in a network, such as computers in a laboratory at a university, or office computers which share resources.

6. These "areas" may be referred to by a variety of names, such as forums, special interest groups (SIGs), conferences, rooms, newsgroups, etc.

7. Anyone with as little as a few hundred dollars can set up and run his or her own BBS. One publisher even puts out "The Complete Electronic Bulletin Board Starter Kit." This book not only explains how to design, set up, install, and fine-tune a bulletin board to fit individual needs, but it also includes the necessary computer software.

8. Because of the way a BBS is accessed, some have national or international reach. The international aspects of computer information systems are beyond the scope of this article, although with the increasingly international reach of telecommunications it is important to keep in mind that some computer systems may be used by people in other countries as easily as they are used by people in their home country. Bulletin Board Systems originally started on a small scale, used by local computer "hackers" to exchange information among themselves.

The term *hacker* is used in a number of different ways. It was originally used to refer to someone who uses his or her computer knowledge to break into other computer systems. *See* Jensen, *An Electronic Soapbox: Computer Bulletin Boards and the First Amendment*, 39 FED. COM. L.J. 217 n.50 (1987).

With the rise of national and international computer networks, BBSs are becoming more accessible to the general public around the world. Some countries already provide their citizens easy access to state-endorsed computer information systems. The world leader in this area is France, which has provided its "Minitel" service since 1982. Conhaim, *Maturing French Videotext Becomes Key International Business Tool*, 9 INFO. TODAY 28 (1992). Minitel had grown to a system of about six million terminals by the end of 1991, and includes access to over 16,000 information services. Wilson, *The Myths and Magic of Minitel; France's Minitel Videotex Service*, TELEPHONY, Dec. 2, 1991, at 52.

Another use for Bulletin Board Systems is in sending electronic mail, or *E-mail* as it is commonly called. Electronic mail is a message sent from one computer user to another, either between users on the same computer, or between users on different computers connected together in a network. Electronic mail is different from regular mail in three important ways. First, E-mail is provided by private parties and, thus, is not subject to government control under the postal laws.[9] However, it is under the control of the System Operator (often called the *SYSOP*) of the Bulletin Board System.

This gives rise to the second issue—privacy. Unlike the U.S. mail, electronic mail is almost always examinable by someone other than the sender and the receiver. By necessity, the communications provider may not only have access to all mail sent through the computer system, but may also have to keep copies (or "backups") in case of system failure.[10]

Third, E-mail is interactive in nature and can involve almost instantaneous communication, more like a telephone than regular mail,[11] so much so that regular users of E-mail often refer to the U.S. mail as "snail mail."

Many Bulletin Board systems permit the uploading and downloading of files.[12] A BBS providing a section of files for its users to download can distribute almost any type of computer file. These files may consist of text, software, pictures, or even sounds. Multiple user Bulletin Board Systems are also frequently used for their "chat" features, allowing a user to talk to other users who are on-line (connected to the host computer) at the same time.[13]

---

9. Kastenmeier, et al., *Communications Privacy: A Legislative Perspective*, 1989 WIS. L. REV. 715, 727 (1989) [hereinafter *McGiverin*].

10. *Id.*

11. *Id.*

12. *Downloading* entails transferring files from the computer on which the BBS runs to the user's computer, and *uploading* is the reverse.

13. This operates as a way to get information more directly from other people and even to meet new friends. In fact, for some people a BBS is a major social outlet, allowing communication on equal terms without first impressions being formed by physical appearances. Some people have even decided to get married to other users, based solely on the messages they have exchanged. Johnston, *Looking for Log-on Love*, GANNETT NEWS SERV., Mar. 25, 1992 (available in LEXIS, Nexis Library, current file). Others are not looking for information or casual conversation, but rather for "net sex." Chat features can be used much like telephone 900 number dial-a-porn services. Before cracking down on them, the French Minitel system determined that sex-oriented messages constituted nearly twenty percent of the usage of its conferencing system. Markoff, *The Nation; The Latest Technology Fuels the Oldest of Drives*, N.Y. TIMES, Mar. 22, 1992, § 4, at 6.

2. *Teletext and Videotex or Videotext*

Another kind of computer information system is *Teletext*,[14] a one-way distribution system, generally run over a cable television system. It sends out a continually repeating set of information screens. By using a decoder, a user can select which screen he or she wants. The decoder then "grabs" the requested screen and displays it as it cycles by. Since Teletext is only a one-way service, a user can only read the information the service has available for his or her reading. There is no way for the user to contribute his or her own input to the system.

More advanced than Teletext is *videotex*[15] (often called *videotext*).[16] Videotex is a two-way service usually employing a personal computer as a terminal. When provided via a telephone, videotex is basically the same as any other computer information system discussed in this article, so the terms "videotex" and "computer information system" are used synonymously for ease of discussion.

3. *Information Distribution Systems*

Computers are used frequently for distributing information of various types. One common type of information distribution system is the database service.[17] This service allows the user to enter a variety of "search terms" to look through the information the service has collected.[18]

Another type of information distribution system is the "file server." A *file server* (or just "server") is a storage device, such a disk drive or CD-ROM, hooked up to a computer network, which lets any computer connected to the network access the files contained on the server. These files can consist of virtually anything, ranging from software to news articles distributed by a "news server." While file servers may be found as part of another computer information system, the server itself is used only for storing and retrieving files.[19]

---

14. *See generally* Neustadt, *Symposium. Legal issues in Electronic Publishing: 1. Background—The Technology*, 36 FED. COM. L.J. 149 (1984).

15. *Id.*

16. The final "t" is often left off because on many computers, filenames are limited to eight characters. *See A Glossary of Computer Technology Terms*, AM. BANKER, Oct. 25, 1989, at 10.

17. Examples include WESTLAW, LEXIS, DIALOG, ERIC, and the local library's card catalog.

18. Some of these services are quite large, and may contain the whole text of books and periodicals, although some may contain only citations, requiring the user to look elsewhere to find the actual material desired. These services differ significantly in their degree of complexity, for example, in the types of search terms they will allow.

19. On large networks, such as the Internet, there are even databases, called "archies," which index the file servers available on the network. They have small descriptions of available software, and give a listing of what machines on the network have the file avail-

4. *Network*

A *network* is a series of computers, connected often by special types of telephone wires.[20] Many networks are conduits allowing a user to call up a remote computer from a personal computer or terminal.[21] Many networks allow a much broader range of uses—such as sending E-mail and more interactive forms of communication between machines,[22] transferring computer files, and providing the same remote access and use that the simpler networks allow.[23]

Some of these networks are so sophisticated and far-reaching that they provide an ideal communications medium for the computer literate. They can be used not only for personal E-mail, but they are also used for a number of special kinds of electronic publishing.[24]

B. Issues Involved

Computer information systems present a variety of legal issues. Whenever a new form of communication emerges, there is a concern that, along with legitimate users, will come some abusers. Just as a bulletin board system can be used for political debate, it can also be used as an outlet for defamation. How should this be treated? Who is liable? The user who originally posted the defamation, or the system operator

---

able. Emtage, *What is 'Archie,'* 1 Effector Online, Oct. 18, 1991, (Electronic Frontier Foundation, available over the Internet by anonymous FTP from FTP.EFF.ORG).

20. C. Condon and the Yale Computer Center, Bitnet Userhelp (1988) (available over Bitnet by sending the command "get bitnet userhelp" to NETSERV-BITNIC).

21. Some of the major networks are Tymnet, Sprintnet, and specifically for WESTLAW and LEXIS users, there is Westnet and Meadnet.

22. An example of such interactive communication is the UNIX "Talk" command, which allows a person to talk instantaneously with a remote user. Both users can type simultaneously; one user's text appears on the top of his or her computer screen while the other user's text appears on the bottom.

23. Some examples of these more full-service networks are the Internet, Bitnet, and ARPANET.

24. One such special use is the electronic forum, basically an automated mailing list. A message is sent to a "Listserver," where it is automatically distributed to other people on its electronic mailing list. A *Listserver* is an automated computer mailing program running out of a computer account. Mail is sent to the account and the Listserver redistributes the message. The people on the list then receive the message as E-mail. They can respond by sending a reply back to the Listserver, which then distributes that message to its list, including the first message sender. This works, in effect, like a group of people standing around discussing a topic, though some people are left behind in the discussion if they do not log on to read their mail regularly. Bitnet Userhelp, *supra* note 19.

A similar type of electronic publication is the *electronic digest*. In this situation, a message is sent to the Listserver, but, instead of being automatically sent out, it is held. A "moderator" then sorts through and edits the material for distribution to the people on the digest's mailing list. *Id.* The most formal type of electronic publishing is the electronic magazine or journal, often called the *Ejournal*. These are "real" magazines, just like print magazines, but they are distributed electronically, rather than in hard copy. *Id.*

who controls and provides the forum? Currently, these are hotly debated issues.

Whenever a new communications medium is developed, there is a risk it will be used to deliver material which society frowns upon, such as obscene or indecent data. Computer information systems allow the distribution of this material in the forms of text, picture and sound. The systems can also be used to provide an outlet for information aiding the criminal world.

One major use for computer information systems is transferring files. In fact, that is the whole purpose of services such as file servers. Legal issues arise when these files contain copyrighted material, such as text, pictures, sounds, or computer software, since such transfers may violate copyright law.

A growing threat to computer users is the *computer virus*. The Computer Virus Industry Association reported that in 1988, nearly 90,000 personal computers were affected by computer viruses.[25] Viruses can be distributed via computer information systems, both consciously and unconsciously. They can be put into a system by someone intending to cause harm, or they can be innocently transferred by a user who has an infected disk.[26]

Another issue for users and system operators of computer information systems is *privacy*. With society becoming increasingly computerized, people need to be made aware of how secure their stored data and electronic mail really is. The Fourth Amendment to the United States Constitution reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized."[27] Yet, how does this amendment apply to Cyberspace, when Cyberspace is a vague, ethereal place with no readily identifiable boundaries, where a "seizure" may not result in the loss of anything tangible, and may not even be noticed?

In all of these cases, questions exist as to who is liable. If SYSOPs are not made aware of the legal issues they may face in running a computer system, they may either fail to reduce or eliminate harm when it is within their power to do so, or they may unnecessarily restrict the services provided out of fear of liability.

---

25. Stover, *Viruses, Worms, Trojans, and Bombs: Computer "Infections,"* POPULAR SCI., Sept. 1989, at 59.

26. Some people consider computer viruses such a threat that Lloyd's of London even offers an insurance policy that specifically covers viruses.

27. U.S. CONST., amend. IV.

C. Legal Analogies

Liability for illegal activities in Cyberspace is affected by how the particular computer information service is viewed. Some services allow one entity to deliver its message to a large number of receivers. In this regard the service acts like a publisher. Some theorists already refer to computer networks as "the printing presses of the 21st century."[28] Many publishers use BBSs to supplement their printed editions either by providing stories and information or by providing additional computer information services on a BBS.[29]

However, other services are more like common carriers than publishers. Networks just pass data from one computer to another—they do not gather and edit data. Still other services are more akin to broadcasting than common carriage. This is because computer services can be provided by sending data over the airwaves, offering the same services available from computers networked together by wire. Computer services can also be used to allow many entities to deliver their messages simultaneously to many other entities. In this way, computer information systems are likened to traditional public fora, such as street corners or community bulletin boards.

None of these analogies is especially useful taken individually. Each is accurate in describing some situations, but lacking in describing others. There is a tendency to look at a service and give it a label, and then regulate it based on its label. This labeling works well in some instances; but, when a service has a number of communication options, such as a BBS that provides a series of bulletin boards, E-mail, and a chat feature, and makes available electronic periodicals in the BBS's file system, one analogy is insufficient. To regulate computer information systems properly, lawyers, judges, and juries need to understand computer information systems and how they work.

II. CURRENT REGULATORY ENVIRONMENT

The current regulatory environment governing computer information systems is somewhat confused because of the multiplicity of means which can be employed in regulating a wide variety of dissimilar services. The Federal Communications Commission, which regulates broadcasters and common carriers providing electronic data, considers computer information systems to be "enhanced" services, and, therefore,

28. M.I.T. Professor Ithiel de Sola Pool, *quoted in* Markoff, *Some Computer Conversation Is Changing Human Contact*, N.Y. Times, May 13, 1990, § 1 at 1.

29. *"Fred The Computer": Electronic Newspaper Services Seen as "Ad-ons,"* Com. Daily, Apr. 10, 1990, at 4.

not regulated by the F.C.C.[30] However, some specific aspects of computer information systems are governed by existing case law and statutes.

Let us start with a hypothetical situation. The Data Playground is a large, full service bulletin board system. In the BBS's message system one of the fora, called the Sewer, is set aside for the users as a place to blow off some steam and express their anger at whatever they feel like complaining about. Samantha Sysop, the bulletin board operator, feels such a forum is necessary. She feels that without it, frustrated users will leave unpleasant messages in the other fora which are meant for rational discussions of serious topics. By providing the Sewer, users who get upset with other users or with life in general can "take their problem to the Sewer." Because she is unsure of any liability for posts in the Sewer which get too heated, she posts a disclaimer, which can be seen the first time a user posts in or reads the Sewer, which states that the SYSOP disclaims all liability for anything that is said in the Sewer. Samantha Sysop reads the posts left in the Sewer, and once in a while posts a message there herself. One day, a user, Sam Slammer, leaves the following message in the Sewer:

> From: Sam Slammer
>
> I am sick and tired of logging onto this damned bulletin board and seeing that damn user Dora Defamed here. She is always here. However, at least if she is here it means that she is not still at home beating her young daughter. In fact, her daughter is too good looking to be stuck with a mother like Dora. She should be stuck with someone like me, after all, I really like young girls, and having sex with her would be a real catch. (If anyone would like to see the films of the last little girl I had sex with, leave me mail.) Anyway, Dora: it is a wonder that kid isn't brain damaged, seeing as you are so badly warped. I would really like to do society a favor and kill you before you get the chance to beat any more children. In fact, if anyone is near the computer where Dora is connected to this BBS from, I urge you to go over to her and kill her. Do us all a favor.

This hypothetical post raises a number of issues. In this one post there is potentially defamatory speech, speech advocating lawless action, fighting words, and an admission and solicitation of child pornography.

30. Second Computer Inquiry (Amendment of Section 64.702 of the Commission's Rules and Regulations, Notice of Inquiry and Proposed Rulemaking), 61 F.C.C.2d 103 (1976). *See also* Second Computer Inquiry, Final Decision, 77 F.C.C.2d 384, 420-21 (1984), which talks directly about BBSs as enhanced services.

A. DEFAMATION

Defamation can occur on a computer information system in a number of forms: posts on a bulletin board system, like the one in the Sam Slammer hypothetical can be defamatory, as can electronic periodicals; file servers and databases can distribute defamatory material; and E-mail can contain defamatory statements. Defamation can even be distributed in the form of a scanned photograph.[31] But what is defamation, and what risks and obligations does it present to a system operator?

Defamation occurs in two form, libel and slander. The difference between these two forms of defamation is often not apparent, based on a common sense approach, rather it is solely a matter of form and "no respectable authority has ever attempted to justify the distinction on principle."[32] With the rise of new forms of technology, which confuse the distinction between libel and slander, many courts have advocated the elimination of the distinction.[33]

Speech on a computer information system has more of the characteristics of libel than slander. Most courts have argued, based on libel cases, that messages appearing on computer information systems are libel and not slander; often just calling it by the generic term "defamation."[34]

Slander is publication in a transitory form—speech, for example, can be slanderous.[35] *Libel*, on the other hand, is embodied in a physical, longer lasting form, or "by any other form of communication that has the potentially harmful qualities of written or printed words."[36] Written or printed words are considered more harmful than spoken words because they are deemed more premeditated and deliberate. For example, Sam Slammer had to sit down at a keyboard and compose his post; it is not a matter of a comment carelessly made in a fit of anger. Printed words are also longer lasting, because they are put in a form in which they can serve to remind auditors of the defamation, while the spoken word is gone once uttered.[37]

Had Sam Slammer accused Dora Defamed of child abuse in person, the statement would be fleeting; on the BBS, it is stored for viewing by any user who decides to read what posts have been left in the Sewer. For days, weeks, or months people can read Sam's statement unless Samantha Sysop removes it. Any user can save a copy of the post on his

31. *See* Sarno, *Libel and Slander: Defamation by Photograph*, 52 A.L.R.4th 488.
32. Restatement (Second) of Torts § 568, comment b (1989).
33. *Id.*
34. *See, e.g.*, Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749 (1985).
35. Restatement (Second) of Torts § 568(2) (1989).
36. *Id.* § 568(1).
37. *See* Tidmore v. Mills, 33 Ala. App. 243, 251, 32 So. 2d 769 (1947).

or her own computer, and can distribute it, verbatim, to anyone else, with Sam's name right at the top. Text on a computer screen shares more traits with libel than with slander. Computer text appears as printed words, and it is often more premeditated than spoken words. Computer text can be called up off of a disk as many times as is needed. The message can even be printed out and the text can be more widely circulated than the same words when they are spoken.

In its barest form, libel is the publication of a false, defamatory and unprivileged statement to a third person as written or printed words, or any other form of communication that has the potential harmful qualities characteristic of written or printed words.[38] "Defamatory" communication is defined as communication that tends to harm the reputation of another so "as to lower him [or her] in the estimation of the community or to deter third persons from associating or dealing with him [or her]."[39] Actual harm to reputation is not necessary for a statement to be defamatory, and the statement need not actually result in a third person's refusing to deal with the object of the statement; rather the words used must be likely to have such an effect.[40] For this reason, if the person defamed already looks so bad in the eyes of the community that his or her reputation could not be made worse, or if the statements are made by someone who has no credibility, there will not be a strong case for defamation.[41]

"Community" does not refer to the entire community, but rather to a "substantial and respectable minority" of the community.[42] Even more specifically, the community is not necessarily seen as the community at large, but rather as the "relevant" community.[43] This means, for example, that one could post a defamatory message on a bulletin board system defaming another user and be subject to a libel suit, even though only other BBS users see the post.

In the hypothetical, we do not know whether Sam's accusations of child beating are true. If they are, Sam would have a defense against a charge of libel. (Whether or not the speech is privileged will be discussed shortly.) The comment is being "published" to any other BBS user who reads the message he has left publicly, and as already discussed, the computer message has the same harmful qualities as a message written

38. Restatement (Second) of Torts §§ 557-59 (1989).

39. *Id.* § 559.

40. *Id.*, comment d.

41. *Id.*

42. *Id.*, comment e.

43. *See, e.g.*, Ben-Oliel v. Press Publishing Co., 251 N.Y. 250, 167 N.E. 432 (1929). This case involved a newspaper article on Palestinian art and custom which was mistakenly credited to the plaintiff, an expert in the field. The article contained a number of inaccuracies that, while still impressive to the lay reader, would embarrass the plaintiff among other experts.

and distributed on paper. In fact, Sam's comments are potentially reaching a larger audience than Sam could have reached by simply posting a notice on a bulletin board in the local computer center. The remark about child abuse has the potential for lowering people's estimation of Dora, and could easily encourage people to avoid associating with her. Even if people do not avoid Dora because of the remark, in a defamation suit it is sufficient that the statements have the potential to have that effect, and here they clearly do. The community at issue here is not the world at large, but rather a substantial and respectable minority of the "relevant" community. Bulletin Board Systems can give rise to a close knit group of users. Here, she is being attacked in a public forum in front of the whole community of users.

This raises another issue: Can a real live person sue for defamation that occurred to a fictitious name or a persona that appears on a computer? If "Dora Defamed" was not the BBS user's real name, could the real user sue Sam Slammer for defaming the user's "Dora" persona on the BBS? In a bulletin board community, unless users know each other in real life away from the computer, the only impression one user gets of another is from how he or she appears on the computer screen. The user in real life may not even be the same sex as the person he or she portrays on the bulletin board system. On the BBS people only know and associate with Dora, not the real person behind the name. When Dora is defamed, in essence so is the person behind the computer representation of Dora. The user is defamed in the eyes of the users behind all of the other BBS personalities that read Sam's post. It should not matter if Dora Defamed is not the user's real identity—a defamation action should still be allowed.

The last issue is whether Dora is being defamed in front of at least a "substantial and respectable" minority of the relevant community. This hinges on who reads the Sewer forum. If the Sewer is widely read, a defamation suit will be more likely to succeed than if the Sewer is largely ignored.

Because defamation involves speech, defamation raises serious First Amendment concerns. Just because speech is defamatory, does not mean that it is unprotected. Analysis is based on who is party to the defamation. In our hypothetical, the relevant parties are Sam and Dora. Constitutional protection was found for some types of defamation in *New York Times v. Sullivan*.[44] This case involved an advertisement taken out in a newspaper expressing grievances with the treatment of blacks in Alabama. An elected city commissioner sued, claiming that the statements made in the advertisement defamed him and that the advertisement contained some inaccuracies. Justice Brennan argued that the

44. 376 U.S. 254 (1964).

case should be considered "against the background of a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials."[45] The court went on to hold that, because one of the main purposes of the First Amendment was to preserve debate and critical analysis of the affairs of elected officials, any censorship of that speech would be detrimental to society. Because of this, the court said libel laws should be relaxed where the speech pertains to the affairs of elected officials.

Likewise, due to the importance of being able to examine the worthiness of public officials, they felt that speech critical of officials should also be less open to attack on grounds of falsity. False speech that is made known can be investigated, but true speech that the critic worries may be false and may result in a libel suit, will remain undisseminated. Because of the importance of monitoring elected officials, the court held that allowing speech that would aid in the monitoring of elected officials' conduct was more important than protecting officials from potential harm resulting from defamatory speech.

A balance between open debate and freedom from defamation was struck by establishing an "actual malice" standard of liability for the publisher. *Actual malice* is a term of art with a specific meaning in the publishing context. As the court stated:

> The constitutional guarantees require, we think, a federal rule that prohibits a public official from recovering damages for a defamatory falsehood relating to his [or her] official conduct unless he [or she] proves that the statement was made with 'actual malice'—that is, with knowledge that it was false or with reckless disregard of whether it was false or not.[46]

This standard applies to electronic publishing as clearly as it applies to print or speech. SYSOPs and users are freed from liability for defamation carried on computer information systems, as it applies to public officials, so long as the material is not allowed to remain when the SYSOP or user knows of its falsity or has reckless disregard for its truth. Dora, as far as we know, is not a public official. If Dora were a persona on the bulletin board system, and not the user's actual name, and if there is no way for the average user to associate the persona with the real person, then even if "Dora" were defamed and the real user was a public official, it would be questionable as to whether the public official privilege would apply. In this situation, the rationale behind the privilege would not be relevant to the actual facts. Statements about Dora do not reflect on the

45. *Id.* at 270.
46. *Id.* at 279-80.

actual user's abilities to perform his or her official job. If, however, the public official can be linked to the Dora persona, then the basis for privileging statements about public officials does apply to the situation, and Sam Slammers' statement may be privileged, presuming no actual malice was intended.

The *New York Times* standard was expanded in two subsequent cases. *Curtis Publishing Co. v. Butts*,[47] and its companion case, *Associated Press v. Walker*,[48] both involved the defamation of people who did not fit under the "public official" heading, but who were "public figures." The Court held that some people, even though they are not part of the government, are nonetheless sufficiently influential to affect matters of important public concern.[49] The Court defined public figures as "[t]hose who, by reason of the notoriety of their achievements or the vigor and success with which they seek the public's attention, are properly classed as public figures . . ."[50] Because these people have influence in our governance, just as public officials do, the same "actual malice" standard should apply to such public figures.

Here, as in the case of public officials, we do not know who Dora Defamed is. If she is a public figure, Sam's child abuse claim may be privileged; if she is not, he may be liable. Another major case defining the constitutional protection of defamation is *Gertz v. Robert Welch, Inc.*[51] In *Gertz*, a magazine published an article accusing a lawyer of being a "Communist-fronter" and a "Marxist." The article accused the plaintiff of plotting against the police. The plaintiff was a lawyer who played a role in the trial of a police officer who was charged with shooting a boy.[52] The lawyer sued for defamation. The publisher defended based on another exception that the court had made in *Rosenbloom v. Metromedia, Inc.*[53] *Rosenbloom* extended the *New York Times*[54] standard to include not just public officials and public figures, but also private figures who were actively involved in matters of public concern. The *Gertz* Court held that this expansion went too far,[55] and overruled *Rosenbloom*.[56]

The Court in *Gertz* acknowledged that the press should not be held strictly liable for false factual assertions where matters of public interest

47. 388 U.S. 130 (1967).
48. *Id.*
49. *See id.* at 164 (Warren, C.J., concurring).
50. 418 U.S. 323, 342 (1974).
51. *Id.*
52. *Id.* at 326.
53. 403 U.S. 29 (1971).
54. *New York Times*, 376 U.S. 254 (1964).
55. *Gertz*, 418 U.S. at 345.
56. *Id.* at 346.

are concerned.[57] Strict liability would serve to chill the publisher's speech by leading to self censorship where facts are in doubt. This First Amendment interest was balanced against the individual's interest in being compensated for defamatory falsehood.[58] The Court reasoned that private individuals were deserving of more protection than public officials and public figures because the private person does not have the same access to channels of communication,[59] and has not voluntarily exposed himself to the public spotlight.[60] The court held that "so long as they do not impose liability without fault, the States may define for themselves the appropriate standard of liability for a publisher or broadcaster of defamatory falsehood injurious to a private individual."[61]

Courts have not made it very difficult for private people to sue for defamation where no matter of public concern is at issue. In one of the more famous defamation cases, *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*,[62] Dun & Bradstreet was held liable for a credit report made from inaccurate records contained in a database.[63] The court argued that statements on matters of no public concern, especially when solely motivated by profit, did not deserve sufficient First Amendment protection to outweigh the individual's interest in suing for defamation.[64]

In our hypothetical, we must look to the subject of Sam Slammer's defamatory comment to see if it is a matter of public concern. Sam is accusing Dora of "beating her kid." While child abuse may be a matter of public concern, whether Dora is such an abuser is not likely a matter of public concern. Just as peoples' inabilities to pay their debts can be a matter of public concern, as was found in the *Dun & Bradstreet* case,[65] the ability of one particular company to pay its debts is not necessarily a matter of public concern. Child abuse is not the issue in this hypothetical; Dora Defamed's potential child abuse is the issue.

The press has been found to have other privileges—not as the privileges pertain to who is being defamed, but rather as a result of the kind of news the press is reporting. One such privilege is for fair report or "neutral reportage"[66] (which is not an issue in our hypothetical). This

57. *Id.* at 340.
58. *Id.* at 341.
59. *Id.* at 344.
60. *Id.*
61. *Id.* at 347.
62. 472 U.S. 749 (1985).
63. *Id. Cf.* Thompson v. San Antonio Retail Merchants Association, 682 F.2d 509 (5th Cir. 1992).
64. *Dun & Bradstreet*, 472 U.S. at 761-62.
65. *Id.*
66. *See* Edwards v. National Audubon Society, Inc., 556 F.2d 113 (2d Cir. 1977). *See also* Time, Inc. v. Pape, 401 U.S. 279 (1971) (newspaper's coverage of a government report

isolates a reporter from defamatory statements that he or she is reporting. The reason behind this is that even just the fact that some statements were made is a matter of public interest, especially involving sensitive issues, and the public interest is best served by allowing the press to inform people of these statements without the risk of liability.[67] Neutral reporting is privileged, but if the reporter is found not to have lived up to the "actual malice" standard (knowing or careless disregard for the truth), his or her report will not be considered neutral, and the fair report privilege will not apply.

Statements of opinion are also privileged.[68] Protection of opinion is, of necessity, not absolute, however, otherwise "a writer could escape liability . . . simply by using, explicitly or implicitly, the words 'I think'."[69] Sam Slammer cannot defend himself by saying, "Well, I think Dora beats her daughter." The court in *Cianci v. New Times Publishing Co.*[70] succinctly laid out the limits of the privilege:

> (1) that a perjorative statement of opinion concerning a public figure generally is constitutionally protected . . . no matter how vigorously expressed;
>
> (2) that this principle applies even when the statement includes a term which could refer to criminal conduct if the term could not reasonably be so understood in context; but
>
> (3) that the principle does not cover a charge which could reasonably be understood as imputing specific criminal or other wrongful acts.[71]

In the hypothetical, Sam's comment directly accused Dora Defamed of a criminal act. Even if he had stated that he believes that she beats her daughter, unless the statement is clearly one interpretable as an opinion, he still is likely to be held liable for his remark (if it is untrue).

In sum, what all of this means for computer information systems, whether speech on a bulletin board, text in an electronic journal, or on any of the other forms of electronic publication, is that liability may result if the message is libelous. It will not result in liability if the defamation concerns public figures, public officials, or matters of public interest. Communications that defame a user may not constitute defamation to the community at large, but the statements may still give rise to liability

---

which, due to inaccuracies, defamed a public official, could not result in liability unless the newspaper published the story with actual malice); Beary v. West Publishing Co., 763 F.2d 66 (2d Cir. 1985) (publisher who exactly reprinted a court opinion, that the plaintiff argued was defamatory, was held absolutely privileged for any defamatory comments contained in the court's opinion).

67. *Edwards*, 556 F.2d at 119.

68. Cianci v. N.Y. Pub. Co., 636 F.2d 54 (2d Cir. 1980) *modified on denial of reh'g*, Oct. 27, 1980.

69. *Id.* at 64.

70. *Id.* at 54.

71. *Id.* at 64.

if it lowers the opinion of that person in the eyes of the rest of the bulletin board users.

B. Speech Advocating Lawless Action

The First Amendment states that "Congress shall make no law . . . abridging the freedom of speech, or of the press."[72] The First Amendment is one of the most important guarantees in the Bill of Rights, because speech is essential for securing other rights.[73] While the right of free speech has been challenged by the emergence of each new medium of communication, the right of free speech still applies to the new forms of communication, though it is, at times, more restrictive.[74]

An example of such a restriction is the regulation of radio and television by the F.C.C. The rationale for F.C.C. governance is based on spectrum scarcity. Currently, this is not a real issue with computer information systems, but with the rise of packet radio and wireless networks which transmit computer data through the airwaves,[75] the F.C.C. may choose to regulate some aspects of computer information systems.

Some people advocate that with changes in technology, distinctions between different forms of media, such as between electronic and print media, should be eliminated. Instead, one all-encompassing standard should be used.[76] No matter what the standard employed, some forms of speech are currently not allowed on the local street corner or on the local computer screen.

In our Sam Slammer hypothetical, questions arise as to whether his message contains some of this speech which is inappropriate for public consumption. One type of speech not permitted is advocacy of lawless action, as laid out in *Brandenburg v. Ohio*.[77] *Brandenburg* held that the guarantees of free speech and free press do not forbid a state from proscribing advocacy of the use of force or violation of law "where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action."[78] Sam threatened to kill Dora, and he urged others to kill her as well.

An important distinction must be made between mere advocacy and incitement to imminent lawless action—the first is protected speech,

---

72. U.S. Const., amend. I.

73. Legal Overview: The Electronic Frontier and the Bill of Rights (No date) (Electronic Frontier Foundation, available over the Internet by anonymous FTP from FTP.EFF.ORG).

74. *Id.*

75. Kramer, *Wireless Communication Net: Dream Come True; Wireless Distributed Area Networks: The Wide View*, P.C. Week, Mar. 5, 1990, at 51.

76. Legal Overview, *supra* note 73.

77. 395 U.S. 444 (1969).

78. *Id.* at 447.

while the second is not. This distinction is quite important, yet can be blurry, in a computer context. On a Bulletin Board System, for instance, messages may be read by a user weeks after they are posted. It is hard to imagine such "stale" messages as advocating imminent lawless action. In our hypothetical, Sam encourages anyone near the computer Dora is using to kill her. A user who reads the post hours later may no longer have the opportunity to take the requested action, even if so inclined. Dora may be, say, at home (beating her daughter?), and no longer at that computer. The action was advocated, but other users will not be incited to carry out the action because the act would not be possible at the time. An information system with a chat feature, which allows users to talk nearly instantaneously to one another, is, however, altogether different. With such a "chat" feature, it would be possible to make a *Brandenburg* incitement threat.

C. Fighting Words

Another kind of speech not given First Amendment protection is "fighting words." *Fighting words* are "those which by their very utterance inflict injury or tend to incite an immediate breach of the peace."[79] In *Chaplinsky v. New Hampshire* the Court held that fighting words (as well as lewd, obscene, profane, and libelous language) "are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality."[80] The Court further defined fighting words as words that have a direct tendency to provoke acts of violence from the individual to whom the remarks are addressed, as judged not by what the addressee believes, but rather by what a common person of average intelligence would be provoked into fighting.[81]

A message posted on a bulletin board or sent by E-mail could contain fighting words. Dora is being accused of being a child abuser, and in the message someone offers to sexually abuse her young daughter. There is no imminence requirement in *Chaplinsky*[82] as there is in *Brandenburg*.[83] Fighting words can be considered delivered to the addressee when the message is read. Dora will undoubtedly become enraged when she reads Sam's message. When Sam left the message has little bearing on when Dora will be ready to fight.

---

79. Chaplinsky v. State of New Hampshire, 315 U.S. 568, 572 (1942).

80. *Id.* at 572.

81. *Id.* at 573.

82. *Id.*

83. *Brandenburg*, 395 U.S. 444 (1969).

While it is hard to fight with the message sender when he or she may not be nearby or even in the same country, that does not preclude some forms of "fighting." Of course, if the sender of the fighting words is nearby, actual fighting could occur. If the sender of the message is on a computer network, an angered recipient could "fight" by trying to tamper with or otherwise damage the sender's computer account. If Sam had written his post about Samantha Sysop instead of Dora, he could find himself unable to access the bulletin board system, or he may find that his copy of his master's thesis on which he was working is suddenly missing from his computer account.

D. Child Pornography

Some areas of content on computer information systems besides speech are regulated. One of these areas is child pornography. *New York v. Ferber*[84] held that States can prohibit the depiction of minors engaged in sexual conduct. The *Ferber* court gave five reasons for its holding. First, the legislative judgment that using children as subjects of pornography could be harmful to their physical and psychological well-being easily passes muster under the First Amendment. Second, application of the *Miller* standard for obscenity[85] (discussed *infra*) is not a satisfactory solution to the problem of child pornography. Third, the financial gain involved in selling and advertising child pornography provides incentive to produce such material and such activity is prohibited throughout the United States. Fourth, the value of permitting minors to perform/appear in lewd exhibitions is negligible at best. Finally, classifying child pornography as a form of expression outside the protection of the First Amendment is not incompatible with earlier court decisions. The court said "The distribution of photographs and films depicting sexual activity by juveniles is intrinsically related to the sexual abuse of children . . ."[86] and is therefore within the State's interest and power to prohibit.

The Federal government has explicitly addressed child pornography as it pertains to computer communication.[87] Section 2252 of Title 18 of the U.S. Code forbids knowing interstate transportation or reception of visual depictions of minors engaged in sexually explicit conduct. It also forbids transporting or receiving such material by any means, including pictures scanned into a computer, for example.[88]

---

84. 458 U.S. 747 (1982).

85. Miller v. California, 413 U.S. 15 (1973).

86. *Ferber*, 458 U.S. at 759.

87. *See* 18 U.S.C. § 2252 *et seq.*

88. *Id.* § 2252(a)(1).

Pictures can be easily reduced to a computer-readable form. Once in such form, they can be distributed, interstate, over a computer information system. Pictures are put into a computer by a process called "scanning" or "digitizing." Scanning is accomplished by dividing a picture up into little tiny elements called *pixels*. The equivalent can be seen by looking very closely at a television screen or at a photograph printed in a newspaper. The computer examines each of these dots, or pixels, and measures its brightness; the computer does this with every pixel. The picture is then represented by a series of numbers that correspond to the brightness and location of each pixel. These numbers can be stored as a file for access on a bulletin board system or file server or can be transferred over a network.[89]

Computers of course do not differentiate between "innocuous" pictures and pictures that are pornographic. A piece of child pornography can be scanned and distributed by file server, bulletin board, or through E-mail just like any other computer file. If Sam Slammer had received a response from someone interested in seeing the pictures of the last time he had sex with a child, the pictures could easily be scanned into a computer-readable form and distributed over a BBS or computer network. While a computer may not differentiate between subject matter of pictures, the law does—persons responsible for distributing child pornography could be sued for child abuse, and such a suit could result in $50,000 or more in fines and damages.[90] If Sam Slammer did try to distribute the pictures he made of the last time he had sex with a minor, his distribution of those pictures over a computer information system could result in a suit for child abuse.

Another issue raised by section 2252[91] is possession of pornographic material. Anyone who "knowingly possess[es] 3 or more books, magazines, periodicals, films, video tapes, or other matter which contains any visual depiction [of child pornography] that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by means including computer"[92] can be fined and imprisoned for up to five years.[93]

While this requirement of knowledge may insulate some computer information systems such as networks, it clearly does not protect computer users who knowingly traffic in pornographic material stored in computer files. Thus, if Sam were distributing pornographic pictures in

89. *See* Lunin, *An Overview of Electronic Image Information*, OPTICAL INFO. SYS., May 1990, at 114.

90. *See* 18 U.S.C. § 2255.

91. *Id.* § 2252.

92. *Id.* § 2252(a)(4)(B).

93. *Id.* § 2252(b).

and out of his computer account, he could be charged under section 2252 with transporting material used in child pornography. He would probably need to be caught with three pictures in his account at the time, but it is likely that a prosecutor could ask a system operator to look through any back-ups of the computer data that were in Sam's account at an earlier time.

Typically, a system operator will make a backup copy of all of the data stored on a computer system. This is done so that if the computer should malfunction, the information can be restored by use of this backup. Backups are often kept for a while before being erased, in essence freezing all of the users' accounts as they were at a time in the past. If pictures were also found in the backups, a claim could be made that Sam was in possession of these pictures as well. This would be an easy claim to make if San had the ability to ask the SYSOP to recover any of the files that are on these back-ups, but which are no longer in his actual account. Based on the public policy against child pornography, it is likely that an attempt would be made to hold Sam responsible for the knowing possession of any files that were formerly in his account that could still be recovered from the system operator's backups of Sam's data.

As to Samantha Sysop's liability, unless she knew what was stored in Sam's account, it is unlikely that she would be held liable for having child pornography stored on her computer system. Section 2252, as quoted above, contains a knowledge requirement. If Samantha Sysop did not know what was in Sam's account, she would not meet that knowledge requirement. If she had reason to know that Sam had pictures of child pornography in his account, but intentionally turned her back, she could be considered to have constructive knowledge of the presence of the pornographic material on her system, and therefore she could be chargeable with the knowing possession of the material. It is not likely to make a difference that the material is in Sam's account: Sam's account is still on Samantha's computer system which she is responsible for maintaining in a legal manner.

Child pornographers, or pedophiles, may use bulletin board systems and E-mail for more than just storing and transporting pictures. There has been some publicity over bulletin boards being used by pedophiles to contact each other.[94] Law enforcement use of bulletin board systems to track down pedophiles has not resulted in prosecutions of system opera-

94. *See* Doyle, *FBI Probing Child Porn On Computers: Fremont Man Complains of Illicit Mail*, S.F. CHRON., Dec. 5, 1991, at A23. *See also* Howe, *Va. Man Pleads Guilty in Child Sex Film Plot; Computer Ads Led to Youth Volunteer's Arrest*, WASH. POST, Nov. 30, 1989, at C1; Jackson, *Child Molesters Use Electronic Networks; Computer-crime Sleuths Go Undercover*, L.A. TIMES, Oct. 1, 1989, at 20.

tors, but there have been convictions of BBS users who have arranged to make "snuff films" through contacts they have made over a computer.[95] Sam Slammer had better be careful about who is answering his query about child pornography, or he may find that his public solicitation will attract the interest of the police.

E. Computer Crime

Some areas of "computer crime" are regulated. Computer crime is an issue of which computer information system operators should be aware, as they may be on the receiving end at some point. The term *computer crime* covers a number of offenses, such as:

1. the unauthorized accessing of a computer system;
2. the unauthorized accessing of a computer to gain certain kinds of information (such as defense information or financial records);
3. accessing a computer and removing, damaging, or preventing access to data without authorization;
4. trafficking in stolen computer passwords; and
5. spreading computer viruses.

All of these are activities which are often referred to as "hacking."[96]

1. *Computer Fraud*

The first federal computer crime law, entitled the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984,[97] was passed in October 1984.[98] The Act made it a felony to knowingly access a computer without authorization, or in excess of authorization, in order to obtain classified government defense or foreign relations information with the intent or reason to believe that the information would be used to harm the United States or provide an advantage to a foreign nation. Access to obtain information from financial records of a financial institution or in a consumer file of a credit reporting agency was also outlawed. Access to use, destroy, modify or disclose information found in a computer system (as well as to prevent authorized use of any computer used for government business if such a use would interfere with the government's use of the computer) was also made illegal.[99]

---

95. *See* United States v. Lambey, 949 F.2d 133 (1991).

96. *See supra* note 8.

97. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, ch. 21, 98 Stat. 2190 (1984).

98. Griffith, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 Vand. L. Rev. 453, 455 (1990).

99. *Id.* at 460.

The 1984 Act had several shortcomings, and was revised in the Computer Fraud and Abuse Act of 1986.[100] The 1986 act added three new crimes—a computer fraud offense, modeled after federal mail and wire fraud statutes; an offense for the alteration, damage or destruction of information contained in a "federal interest computer"; and an offense for trafficking in computer passwords under some circumstances.[101]

This Computer Fraud and Abuse Act presents a powerful weapon for SYSOPs whose computers have been violated by hackers. It was made even more powerful by the first person charged with its violation. Robert Morris Jr. was charged with releasing a "worm"[102] onto a section of the Internet computer network,[103] causing numerous government and university computers to either "crash" or become "catatonic."[104] Robert Morris is the son of the Chief Scientist at the National Security Agency's National Computer Security Center. His father is also a former researcher at AT&T's Bell Laboratories where he worked on the original UNIX operating system.[105]

Morris claimed that the purpose of his worm program was to demonstrate security defects and the inadequacies of network security, not to cause harm.[106] However, due to a small error in his program, it got out of control and caused numerous computers to require maintenance to eliminate the worm at costs ranging from $200 to $53,000 apiece.[107] District Judge Munson read the Computer Fraud and Abuse Act largely as defining a strict liability crime. The relevant language applies to someone who:

> (5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby
>
> (A) causes loss . . . of a value aggregating $1,000 or more. . . .[108]

---

100. The Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (1988) [hereinafter Computer Fraud Act].

101. Griffith, *supra* note 98, at 474.

102. A *worm* is described *infra.*

103. Martin, *Revenge of the Nerds: The Real Problem with Computer Viruses Isn't Genius Programmers, It's Careless Ones*, 20 PSYCHOL. TODAY, Jan. 1989, at 21.

104. United States v. Morris, 928 F.2d 604, 506 (2d Cir. 1991), *cert. denied*, — U.S. —, 112 S. Ct. 72 (1991).

105. Nelson, *Viruses, Pests, and Politics: State of the Art*, 20 COMPUTER & COM. DECISIONS, Dec. 1989, at 40.

106. *Morris*, 928 F.2d at 504. UNIX is the operating system that many mainframe computers use.

107. *Id.* at 506.

108. 18 U.S.C. § 1030(a)(5)(A).

Judge Munson interpreted this language as requiring intent only to access the computer, not intent to cause actual damage. On appeal, Munson's reading was affirmed,[109] and the Supreme Court refused to hear further appeals.[110]

However, many agree with Morris' lawyer's, Thomas Guidoboni's, interpretation of this reading of the statute. He describes it as "perilously vague" because it treats intruders who do not cause any harm just as severely as computer terrorists.[111] While the Judge's interpretation of the statute makes it a more powerful weapon in a prosecutor's corner, Guidoboni argues that Munson's interpretation violates the sense of fairness that underlies the U.S. criminal justice system, which almost always differentiates between people who intend to cause harm and those who do not.[112] No one seems to argue that what Morris did was right, but many do not agree that he should have been charged with a felony.[113]

The jury in the *Morris* case indicated that the most difficult question was whether Morris' access to the Internet was unauthorized. Defense counsel pointed out that 2 million subscribers had the same access.[114] This indicates a lack of understanding by the jurors of how computer networks work.[115]

2. *Unauthorized Use of Communications Services*

One of the favorite targets of computer hackers is the telephone company. Telephone systems are susceptible to computer hackers' illegal use. By breaking into the telephone company's computer, hackers can then place free long distance calls to other computers. They can also break into telephone companies' computers and get lists of telephone credit card numbers. Trafficking of stolen credit card numbers and other kinds of telecommunications fraud costs long distance carriers about $1.2 billion annually.[116]

---

109. *Morris*, 328 F.2d 504 (2d Cir. 1991).

110. *Morris*, — U.S. —, 112 S. Ct. 72 (1991).

111. Guidoboni, *What's Wrong With the Computer Crime Statute?: Defense and Prosecution Agree the 1986 Computer Fraud and Abuse Act is Flawed but Differ on How to Fix It*, COMPUTERWORLD, Feb. 17, 1992, at 33.

112. *Id.*

113. Godwin, *Editorial: Amendments Would Undue Damage of Morris Decision*, 1 EFFECTOR ONLINE, No. 12, Oct. 18, 1991 (Electronic Frontier Foundation, available over the Internet by anonymous FTP from FTP.EFF.ORG).

114. Geneson, *Recent Developments in the Investigation and Prosecution of Computer Crime*, 301 PLI/PAT. 45 at 2.

115. *Id.*

116. Skrzycki, *Thieves Tap Phone Access Codes to Ring Up Illegal Calls*, WASH. POST, Sept. 2, 1991, § 1 at A1.

Distribution of fraudulently procured long distance codes is often accomplished over bulletin board systems, or by publication in electronic journals put out by hackers over computer networks. The major protection for the telephone companies is found in 18 U.S.C. § 1343 (mail fraud).[117] This section prohibits the use of wires, radio or television in order to fraudulently deprive a party of money or property. This statute has been held to include fraudulent use of telephone services.[118]

Presumably, this statute also covers fraudulent theft of computer services when the computer is accessed by wire. Computer information systems that knowingly distribute information aiding in wire fraud could be charged with conspiracy to violate 18 U.S.C. § 1346 (wire fraud),[119] which specifically covers schemes to defraud.

Some state laws also punish theft of local telephone service or publication of telephone access codes.[120]

3. *Viruses*

As pointed out in the introduction,[121] computer viruses are increasingly of concern—both for operators of computer information systems and users of those systems. But what is a virus? A *virus* refers to any sort of destructive computer program, though the term is usually reserved for the most dangerous ones.[122]

Computer virus crime involves an intent to cause damage, "akin to vandalism on a small scale, or terrorism on a grand scale."[123] Viruses can spread through networked computers or by sharing disks between computers.[124] Viruses cause damage by attacking another file or by filling up the computer's memory or by using up the computer's processor power.[125] There are a number of different types of viruses, but one of the factors common to most of them is that they all copy themselves (or parts of themselves).[126] Viruses are, in essence, self-replicating.

Also discussed earlier was a "pseudo-virus," called a *worm*. People in the computer industry do not agree on definitions of what is a worm

---

117. 18 U.S.C. § 1343 (1992).

118. *See, e.g.*, Brandon v. United States, 382 F.2d 607 (10th Cir. 1967).

119. 18 U.S.C. § 1346 (1992).

120. *See, e.g.*, State v. Northwest Passage, Inc., 585 P.2d 794 (Wash. 1978) (en banc).

121. *Supra* text accompanying notes 31-32.

122. Kluth, *Computer Law Symposium. The Computer Virus Threat. A Survey of Current Criminal Statutes*, 13 HAMLINE L. REV. 297 (1990).

123. *Id.*

124. *Computer Viruses: Legal and Policy Issues Facing Colleges and Universities*, 64 W. EDUC. L. REP. 761.

125. *Id.*

126. *Id.*

and what is a virus.[127] Regardless, a worm is a program specifically designed to move through networks.[128] A worm may have constructive purposes, such as to find machines with free resources that could be more efficiently used, but usually a worm is used to disable or slow down computers. More specifically, a worm is defined as "[c]omputer virus programs . . . [which] propagate on a computer network without the aid of an unwitting human accomplice. Worms move of their own volition based upon stored knowledge of the network structure."[129]

Another type of virus is the "Trojan Horse." This is a virus which hides inside another seemingly harmless program. Once the Trojan Horse program is used on the computer system, the virus spreads.[130] The virus type which has gained the most fame recently has been the Time Bomb, which is a delayed action virus of some type. This type of virus has gained notoriety as a result of the Michaelangelo virus. A virus designed to erase the hard drives of people using IBM compatible computers on the artist's birthday.[131] Michaelangelo was so prevalent it was even distributed accidentally by some software publishers when the software developers' computers became infected.[132]

One concern many have about statutes dealing with computer viruses is the fact that the statutes need some kind of intent requirement.[133] Without some sort of intent requirement, virus statutes may be sufficiently overbroad to cover defective computer programs.[134]

What legal remedies are available for virus attacks? Distributing a virus affecting computers used substantially by the government or financial institutions is a federal crime under the Computer Fraud and Abuse Act.[135] If a virus also involves unauthorized access to an electronic communications system involving interstate commerce, the Electronic Communications Privacy Act may come into play.[136] Most states have statutes that make it a crime to intentionally interfere with a computer system. These statutes will often cover viruses as well as other forms of

127. Allman, *Worming My Way; November 1988 Internet Worm*, 7 UNIX REV., No. 1, at 74 (1989).

128. Kluth, *supra* note 122.

129. *Id.* at n.14.

130. *Id.*

131. *Id.*

132. *Electronic Mail Software Provider Reports Virus Contamination*, UPI, Feb. 3, 1992 (available in Lexis, Nexis Library, UPI File).

133. *See* Kluth, *supra* note 122.

134. *Id.*

135. 18 U.S.C. § 1030.

136. 18 U.S.C. § 2510 *et seq.* (discussed *infra*).

computer crime. State statutes generally work by affecting any of ten different areas:[137]

1. Expanded definitions of "property" to include computer data.
2. Unlawful destruction of computer files.
3. Use of a computer to commit, or aid or abet commission of a crime.
4. Crimes against intellectual property.
5. Knowing or unauthorized use of a computer or computer services.
6. Unauthorized copying of computer data.
7. Prevention of authorized use.
8. Unlawful insertion of material into a computer or network.
9. "Voyeurism"—Unauthorized entry into a computer system just to see what is there.
10. Taking possession of or exerting control of a computer or software.

SYSOPs must also worry about being liable to their users as a result of viruses which cause a disruption in service. Service outages caused by viruses or by shutdowns to prevent the spreading of viruses could result in a breach of contract where continual service is guaranteed; however, contract provisions could provide for excuse or deferral of obligation in the event of disruption of service by a virus.

Similarly, SYSOPs are open to tort suits caused by negligent virus control. "[A SYSOP] might still be found liable on the ground that, in its role as operator of a computer system or network, it failed to use due care to prevent foreseeable damage, to warn of potential dangers, or to take reasonable steps to limit or control the damage once the dangers were realized."[138] The nature of "care" still has not been defined by court or statute.[139] But still, it is likely that a court would find that a provider is liable for failure to take precautions against viruses when precautions are likely to be needed. SYSOPs are also likely to be held liable for not treating files they know are infected. Taking precautions against viruses would be likely to reduce the chances or degree of liability.

F. Protection From Hackers

System Operators need to worry about damage caused by hackers as well as damage caused by viruses. While hackers are liable for the damage they cause, SYSOPs may find themselves on the receiving end of a

137. Branscomb, *Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime*, 16 Rutgers Computer & Tech. L.J. 1 (1990).

138. *Computer Viruses*, *supra* note 124.

139. *Id.*

tort suit for being negligent in securing their computer information system. For a SYSOP to be found negligent, there must first be a duty of care to the user who is injured by the hacker.[140] There must then be a breach of that duty[141]—the SYSOP must display conduct "which falls below the standard established by law for the protection of others against unreasonable risk of harm."[142] Simply put, the SYSOP must do what is generally expected of someone in his or her position in order to protect users from problems a normal user would expect to be protected against. Events that the SYSOP could not have prevented—or have foreseen and planned for—will not result in liability.[143]

A SYSOP's duty "may be defined as a duty to select and implement security provisions, to monitor their effectiveness, and to maintain the provisions in accordance with changing security needs."[144] SYSOPs should be aware of the type of information stored in their systems, what kind of security is needed for the services they provide, and what users are authorized to use which data and which services. SYSOPs also have a duty to explain to each user the extent of his or her authorization to use the computer information service.[145]

The same analysis applies to operator-caused problems. If the SYSOP accidentally deletes data belonging to a user or negligently maintains the computer system, resulting in damage, he or she would be liable to the user to the same extent as he or she would be from hacker damage that occurred due to negligence.

G. Privacy

Privacy has been a concern of computer information system providers from the very beginning. With the speed, power, accessibility, and storage capacity provided by computers comes the tremendous potential to infringe on people's privacy. It is imperative that users of services such as electronic mail understand how these services work, i.e., how private the user's communications really are, and who may have access to the user's "personal" E-mail. The same is true for stored computer files. Just as important, System Operators should be aware of what restrictions and requirements exist to maintain users' privacy expectations.

---

140. W. Keeton, Prosser & Keeton on the Law of Torts § 30(1), at 164 (5th ed. 1984).

141. *Id.* § 30(2), at 164.

142. *Id.* § 31, at 169.

143. *Id.* § 29, at 162.

144. Massingale & Borthick, *Risk Allocation for Computer System Security Breaches: Potential Liability for Providers of Computer Services*, 12 W. New Eng. L. Rev. 167, 187 (1990).

145. *Id.* at 188-89.

1. *Pre-Electronic Communications Privacy Act of 1986*

One of the most significant cases establishing privacy for electronic communications was *Katz v. United States*.[146] *Katz* involved the use of an electronic listening device ("bug") mounted on the outside of a public telephone booth. The government (which placed the bug) figured that because the bug did not actually penetrate the walls of the booth and was not actually a "wire tap," there was no invasion of privacy. However, Justice Stewart argued that the bug was an unlawful search and seizure in violation of the Fourth Amendment.[147] The court held that "the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection [citations omitted]. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[148]

The decision in this case is also understood to say that if a person does not have a reasonable expectation of privacy, there is, in fact, no Fourth Amendment protection. The person must have a subjective expectation of privacy and, to be reasonable, it must be an expectation that society is willing to recognize as reasonable.[149] For example, most people have a reasonable expectation that calls made from inside a closed telephone booth will be private. What this means for computer users is that, because the computer operator has control over the system and can read any messages, the user cannot reasonably protect his or her privacy. If there is no reasonable expectation of privacy, there can be no violation of privacy, and therefore, no Fourth Amendment claim.[150]

Statutory protection of the right to privacy was originally provided by the federal wiretap statute.[151] However, this statute affected only "wire communication," which is limited to "aural [voice] acquisition."[152] In *United States v. Seidlitz*,[153] the court held that interception of computer transmission is not an "aural acquisition" and, therefore, the Wiretap Act provided no protection. Even if the Act did cover transmission, it still does not cover stored computer data.[154] This does not result in significant or comprehensive protection of E-mail or stored data.

---

146. Katz v. United States, 389 U.S. 347 (1967).

147. U.S. CONST., amend. 4.

148. Katz, 389 U.S. at 351.

149. *See id.* at 347. *See also* California v. Ciraolo, 476 U.S. 207 (1986).

150. *See* Hernandez, Computer Electronic Mail and Privacy (distributed by Electronic Frontier Foundation, available over the Internet by anonymous FTP from FTP.EFF.ORG).

151. 18 U.S.C. § 2510 (1992).

152. *See* Hernandez, *supra* note 150.

153. United States v. Seidlitz, 589 F.2d 152, 157 (4th Cir. 1978), *cert. denied*, 441 U.S. 922 (1979).

154. *See* Hernandez, *supra* note 150.

2. *Electronic Communications Privacy Act of 1986*

> Prior to the passage of the Electronic Communications Privacy Act, communications between two persons were subject to widely disparate legal treatment depending on whether the message was carried by regular mail, electronic mail, an analog phone line, a cellular phone, or some other form of electronic communication system. This technology-dependent legal approach turned the Fourth Amendment's protection on its head. The Supreme Court has said that the Constitution protects people, not places, but the Wiretap Act did not adequately protect all personal communications; rather, it extended legal protection only to communications carried by some technologies.[155]

The Federal Wiretap Act was displaced by the Electronic Communications Privacy Act of 1986.[156] The Electronic Communications Privacy Act deals specifically with the interception and disclosure of interstate[157] electronic communications,[158] and the Act functions as the major sword and shield protecting E-mail. It works both to guarantee the privacy of E-mail and also to provide an outlet for anyone who will not respect that privacy.

The statute provides in part that "any person who . . . intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication"[159] shall be fined or imprisoned.[160] The intentional disclosure or use of the contents of any wire, oral, or electronic communication that is known or could reasonably be known to have been intercepted in violation of the statute is prohibited.[161] This largely guarantees the privacy of E-mail as well as data transfers over a network or telephone line going to or from a computer information system. In essence, E-mail cannot legally be read except by the sender or the receiver; even if someone else actually intercepted the message. Further disclosure or use of the message contents by any party, other than the message sender and its intended recipient, is prohibited if the intercepting party knows or has reason to know that the message was illegally intercepted.

Section 2 of the Electronic Communications Privacy Act[162] provides an exception for SYSOPs and their employees to the extent necessary to manage properly the computer information system:

---

155. Kastenmeyer, *Communications Privacy: A Legislative Perspective*, 1989 WIS. L. REV. 715, 720 (1989) (footnotes omitted).

156. 18 U.S.C. § 2510 *et seq.* (1992).

157. *Id.* § 2510(12).

158. *Id.* § 2511.

159. *Id.* § 2511(1)(a).

160. *Id.* § 2511(4).

161. *Id.* § 2511(1)(c).

162. *Id.* § 2511(2)(a)(i).

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of rights or property of the provider of that service, except that a provider of a wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.[163]

Electronic communication system is defined as "any wire, radio, electromagnetic, photo optical or photoelectric facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."[164] Further exceptions are made for SYSOPs of these systems when the originator or addressee of the message gives consent;[165] when the message is being given to another service provider to be further forwarded towards its destination;[166] where the message is inadvertently obtained by the SYSOP; when the message appears to pertain to a crime; when the divulgence is being made to a law enforcement agency;[167] or where the message is configured so as to be readily accessible to the public.[168]

It is worth noting that this section also applies to broadcast communications as long as they are in a form not readily accessible to the general public (with some exceptions).[169] This will probably cover the up-and-coming technologies of radio-WANS (Wide Area Networks—computer networks which link computers by radio transmission rather than wires), and also packet radio. These technologies are especially likely to be covered by the statute if data is transmitted using some sort of encryption scheme.[170]

For law enforcement agencies to intercept electronic communications, they must first obtain a search warrant by following the procedure laid out in section 2518 of this Act.[171] The statute does not prohibit the use of pen registers or trap and trace devices.[172] The warrant require-

163. *Id.*
164. *Id.* § 2510(14).
165. *Id.* § 2611(3)(b)(ii).
166. *Id.* § 2511(3)(b)(iii).
167. *Id.* § 2511(3)(b)(iv).
168. *Id.* § 2511(3)(b)(i).
169. *Id.* § 2511.
170. Encryption is in essence a coding of the data so it cannot be understood by anyone without the equipment or knowledge necessary to decode the transmission.
171. *See id.* § 2518.
172. *Id.* § 2511(2)(h)(i). A pen register is a device which records the telephone numbers called from a specific telephone; a trap and trace device records the phone originating calls to a specific telephone.

ment makes it harder for law enforcement officials to get at the contents of the communications, but does not substantially impede efforts to find out who is calling the computer information system.

3. *Access to Stored Communications*

Section 2511 of the Electronic Communications Privacy Act concerns the interception of computer communications. Section 2701 of the Act prohibits unlawful access to communications which are being stored on a computer.[173] The section reads, in part, "[W]hoever—(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system"[174] shall be subject to fines and/or imprisonment, or both.[175] Like section 2511,[176] this section includes provisions prohibiting the divulgence of the stored messages.[177] Importantly, while this statute allows law enforcement agencies to gain access to stored communications, subject to a valid search warrant,[178] it does specifically allow the government to permit the system operator to first make backup copies of stored computer data, so that the electronic communications may be preserved for use outside of the investigation. Such a statute is needed because the government often takes the stored data to sort through during the course of its investigation.

4. *Privacy Protection Act of 1980*

It is possible that computer information systems will be protected under the Privacy Protection Act of 1980.[179] The Privacy Protection Act immunizes from law enforcement search and seizure any "work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate commerce."[180] This statute was passed to overturn the decision in *Zurcher v. Stanford Daily*,[181] a case which held that a newspaper office could be searched, even when no one working at the paper was suspected of a crime. The only exceptions to the law's prohibition on searches of publishers are the

173. *Id.* § 2701 *et seq.*
174. *Id.* § 2701(a).
175. *Id.* § 2701(b).
176. *Id.* § 2511.
177. *Id.* § 2702.
178. *See id.* § 2703.
179. 42 U.S.C. § 2000aa.
180. *Id.* § 2000aa(a).
181. 436 U.S. 547 (1978).

following: probable cause to believe that the person possessing the materials has committed or is committing the crime to which the materials relate,[182] or the immediate seizure is necessary to prevent the death or serious injury to a human being.[183] Based on the list of types of "publishers" covered by this statute, electronic publishers should fall under this section, but courts have yet to construe this statute as it relates specifically to computer information systems, though they may very soon.

One case currently is pending which may succeed in applying this law to computer bulletin board systems. The case involves a Secret Service raid of Steve Jackson Games, and it is a good case study in law enforcement violations of electronic data privacy.[184] Steve Jackson Games is a small publisher of fantasy role-playing games in Texas.[185] The company also ran a BBS to gain customer feedback on the company's games. The Secret Service took all of the company's computers, both their regular business computers and the one on which they were running the company's BBS (private electronic mail and all). They also took all of the copies of their latest game, GURPS Cyberpunk, which one of the Secret Service agents referred to as "a handbook for computer crime."[186]

The raid by the Secret Service caused the company to temporarily shut down. Steve Jackson Games also had to lay off half its employees. The release of the game was delayed for months, since the Government took all of the word processing disks as well as all of the printed drafts of the game.[187] The Electronic Frontier Foundation, which provided legal counsel for Steve Jackson, likened the Secret Service's action to an indiscriminate seizure of all of a business's filing cabinets and printing presses.[188] Since the *Pentagon Papers* case was decided in 1971,[189] the Supreme Court would not have allowed such a seizure if a more conventional publisher's rights had been at stake.

In the search warrant, which was sealed at the government's request for seven months, the government neglected to mention to the magistrate that Steve Jackson Games was a publisher. The Secret Service did mention that they did not suspect Steve Jackson Games of any

182. 42 U.S.C. § 2000aa(a)(1).

183. *Id.* § 2000aa(a)(2).

184. Steve Jackson Games v. United States Secret Service (pending in U.S. District Court, W.D. Tex. 1993).

185. Kapor, *Civil Liberties in Cyberspace; Computers, Networks and Public Policy*, SCI. AM., Sept. 1991, at 158.

186. *Id.*

187. Legal Case Summary, May 10, 1990 (Electronic Frontier Foundation, available over Internet by anonymou-FTP from FTP.EFF.ORG).

188. *Id.*

189. New York Times v. United States, 403 U.S. 713 (1971). This case involved a suit over documents that had been stolen from the Pentagon and were later abstracted and published. The government sought to prevent their publication.

wrongdoing, rather, the Secret Service suspected one of the company's employees.[190] Steve Jackson Games was raided because one of its employees ran a BBS out of his home—one out of a possible several thousand around the country that distributed the electronic journal "Phrack," in which a stolen telephone company document was published. The document contained information which was publicly available in other forms.[191] The employee was also accused of being a part of a fraud scheme, the fraud being the explanation in a two line message what Kermit is—a publicly available communications protocol.[192]

The taking of the bulletin board by the Secret Service constitutes a violation of the Privacy Protection Act of 1980.[193] With the bulletin board went the electronic mail. Inspection of stored E-mail violates the Electronic Communication Privacy Act's stored communications provisions.[194] The raid on Steve Jackson Games was only one part of Operation Sundevil, the government's attempt to crack down on computer hacking. Operation Sundevil "seized more than forty computers and 23,000 data disks from teenagers in fourteen American cities, using levels of force and terror which would have been more appropriate to the apprehension of guerrillas than barely post-pubescent computer nerds."[195] The Steve Jackson Games case will undoubtedly have a large impact in the way the law views computer bulletin boards.

H. Obscene and Indecent Material

Computer information systems can contain obscene or indecent material in the form of text files, pictures, or sounds (such as the sampled recording of an indecent or obscene text). Different degrees of liability depend on which legal analogy is applied to computer information systems. Differences in regulation based on medium are a result of differing First Amendment concerns.[196]

---

190. *Legal Fact Sheet: Steve Jackson Games v. United States Secret Service, et al.*, Effector Online, Vol. 1, No. 4, May 1, 1991 (Electronic Frontier Foundation, available over Internet by anonymous FTP from FTP.EFF.ORG).

191. United States v. Riggs, 743 F. Supp. 556 (N.D. Ill. 1990).

192. *Special Issue: Search Affidavit for Steve Jackson Games*, Computer Underground Dig., Issue 2.11, Nov. 13, 1990 (available over Internet by anonymous FTP from FTP.EFF.ORG).

193. 42 U.S.C. § 2000aa (1992).

194. 18 U.S.C. § 2701 (1992).

195. Barlow, A Not So Brief History of the Electronic Frontier Foundation (available over Internet by anonymous FTP from FTP.EFF.ORG).

196. *See, e.g.*, F.C.C. v. Pacifica Foundation, 438 U.S. 726 (1978).

1. *Obscenity*

The constitutional definition of "obscenity" as a term of art[197] was solidified in *Roth v. United States*.[198] The *Roth* definition asks if the material deals with sex in a manner appealing to prurient interests.[199] This standard was further explained in *Miller v. California*,[200] a case which explored the constitutionality of a state statute prohibiting the mailing of unsolicited sexually explicit material. The court expressed the test for obscenity as:

> whether (a) the average person, applying 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.[201]

The first two prongs of this test have been held to be issues left to local juries, while the last prong is to be determined by the court.[202] Courts have been unwilling to find a national standard for obscenity, and have held that a carrier of obscenity must be wary of differences in definition between the states.[203] This has profound implications for computer information systems which have a national reach. It means SYSOPs must be aware of not only one standard of obscenity, but fifty.

SYSOPs must be aware of the different standards because the Constitution's protection of free speech does not extend to obscenity and that States are free to make laws severely restricting its availability, especially to children.[204] Although States can regulate the availability of obscene material, they cannot forbid the mere possession of it in the home.[205] The justification for this is based on privacy. In the now famous words of Justice Marshall in *Stanley v. Georgia*:[206]

> Whatever may be the justifications for other statutes regarding obscenity, we do not think they reach the privacy of one's home. If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read, or

197. The term "obscene material" is used synonymously with "pornographic material"; *see* Miller v. California, 413 U.S. 15, 20 (1973).

198. Roth v. United States, 354 U.S. 476 (1957).

199. *Id.* at 487.

200. Miller v. California, 413 U.S. 15 (1973).

201. *Id.* at 24.

202. Pope v. Illinois, 481 U.S. 497, 500 (1987); Smith v. United States, 431 U.S. 291 (1977).

203. Hamling v. United States, 418 U.S. 87 (1974).

204. *See, e.g.*, Miller v. California, 413 U.S. 15 (1973); Kois v. Wisconsin, 408 U.S. 2219 (1972).

205. Stanley v. Georgia, 394 U.S. 557 (1969).

206. *Id.*

> what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds.[207]

Stanley has been interpreted as establishing a "zone of privacy" about one's home.[208] Many computer information system users are connected to the system by modem from their homes. Because of this, any pornographic material they have stored on their home computers is protected from government regulation.[209] However, connecting to a remote computer information system entails moving obscene material in and out of this zone of privacy, and therefore may not be insulated from state legislation.[210] Support for this argument comes from *United States v. Orito*,[211] which held that Congress has the authority to prevent obscene material from entering the stream of commerce, either by public or private carrier.[212] While a person's disk drive on his or her computer is analogous to his or her home library, connecting to a computer information system can be seen as analogous to going out to a book store. *Stanley*[213] may protect a person's private library, but "[c]ommercial exploitation of depictions, descriptions, or exhibitions of obscene conduct on commercial premises open to the adult public falls within a State's broad power to regulate commerce and protect the public environment."[214]

2. *Indecent Speech*

Speech which is not considered obscene may qualify as indecent. Indecent speech is protected by the First Amendment, unlike obscene and pornographic material, though it can still be regulated where there is a sufficient governmental interest.[215] Indecent language is that which "describes, in terms patently offensive as measured by community standards . . . sexual or excretory activities and organs . . ."[216] This language comes from *F.C.C. v. Pacifica Foundation, Inc.*,[217] a broadcasting case which upheld the channeling of indecent language into time periods when it was not as likely that children would be in the audience. Discussion of indecent speech will be continued in the analysis of the different legal analogies that may apply to computer information systems.

---

207. *Id.* at 665.
208. Jensen, *supra* note 8.
209. Note that an exception would be made for child pornography, *see supra*.
210. Jensen, *supra* note 8.
211. 413 U.S. 139 (1973).
212. *Id.* at 143.
213. *Stanley*, 394 U.S. at 565.
214. Paris Adult Theatre I v. Slaton, 413 U.S. 49, 59-60 (1973).
215. F.C.C. v. Pacifica Foundation, Inc., 438 U.S. 726 (1978).
216. *Id.* at 732.
217. *Id.*

I. COPYRIGHT ISSUES

1. *Basics of Copyrights*

Text, pictures, sounds and software—all of these can be distributed by computer information systems and all can be copyrighted. The Constitution grants Congress the power to "promote the Progress of Science and Useful Arts, by securing for limited Times to Authors and Inventors the exclusive right to their respective Writings and Discoveries."[218] This power is exercised in the form of the Copyright Act, Title 17 of the U.S. Code.[219]

Section 102 of the Copyright Act allows protection of "original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device."[220] The statute lists several kinds of works as illustrations of types of works which qualify for copyright protection. Relevant to computer information systems, the list includes literary works; pictorial, graphic, and sculptural works; motion pictures and other audiovisual works; and sound recordings.[221]

The "now known or later developed" language allows expansion of copyright coverage to meet any new means of expression, such as those available over a computer information system.[222] In fact, the notes accompanying this code section acknowledge that copyright protection applies to a work "whether embodied in a physical object in written, printed, photographic, sculptural, punched, magnetic, or any other stable form."[223]

The element of fixation is important in the copyright statute. A work which is not fixed is not covered by the statute, and any possible protection must come from local common law.[224] This can lead to some strange results. A live concert cannot be copyrighted under this statute, but if someone records the concert while he or she performs, the concert can then be copyrighted.[225] For computer information systems, this implies that conversations occurring over a computer or network which are not stored on a disk[226] are unprotected by the Copyright Act, but if any

---

218. U.S. CONST., art. I, § 8, cl. 8.

219. Copyright Act of 1976, 17 U.S.C. § 101 *et seq.* [hereinafter Copyright Act].

220. *Id.* § 102(a).

221. *Id.* Other categories include musical works, dramatic works, pantomimes and choreographic works, and architectural works.

222. *See id.* § 101, Historical and Statutory Notes.

223. *Id.*

224. *Id.*

225. *Id.*

226. Data which is not stored on a disk is kept in a computer's "RAM" (Random Access Memory). RAM is a volatile information store where the computer keeps the information it

party to the conversation or the system operator stores the messages, it is then possible to copyright some elements of the conversation.

Copyright protection extends to works of authorship; it does not extend to ideas, processes, concepts, inventions and the like.[227] Distinguishing between works of authorship and processes can at times result in some subtle distinctions. An example of this is computer typefaces or fonts (which can often be found available for downloading on file servers or bulletin board systems). There are two major kinds of type faces, bit-mapped and postscript. Bit-mapped fonts are composed of data describing where points are drawn in order to make out the shape of the letter.[228] Postscript fonts, on the other hand, consist of a computer program which describes the outline of the letter.[229] Digital typefaces are not considered copyrightable, because they are seen as just a copy of the underlying letter design, a process for drawing a representation of a letter, and thus bit-mapped fonts are not copyrightable.[230] Postscript fonts are seen as computer programs—the program is a work of authorship that just so happens to draw letters, and they have been held to be copyrightable.[231]

The Copyright Act gives the copyright holder exclusive rights to his or her works.[232] This allows the author to reproduce, perform, display, or create derivative works as he or she pleases, and to do so to the exclusion of all others.[233] This means a computer information system can distribute only material that is either not copyrighted, or for which the SYSOP has permission to copy. This presents no problem for material the system operator acquires, but two problems exist regarding material that users upload to the computer system.

First, even if the SYSOP sees that the material a user has uploaded is copyrighted, how is the SYSOP to know that permission has not been granted by the copyright holder? Second, copyright notices can be removed by the person posting copyrighted material, in which case the SYSOP may have no way to know if the data is copyrighted.

A SYSOP cannot just ignore a suspicion that a work is copyrighted, because such an act could lead to the conclusion that the SYSOP was a

---

is actively processing. When the computer is turned off, all of this data is lost; thus, anything stored in RAM may be missing the required element of fixation."

227. 17 U.S.C. § 102(b).

228. Von Simon, *Page Turns in Copyright Law with Adobe Typeface Ruling*, COMPUTERWORLD, Feb. 5, 1990, at 120.

229. *Id.*

230. *Adobe Successfully Registers Copyright Claim for Font Program*, COMPUTER LAW., Feb. 1990, at 26.

231. Von Simon, *supra* note 228.

232. 17 U.S.C. § 106.

233. *Id.*

participant in the copyright infringement by allowing the computer file to be distributed on his or her system.[234] There is no intent or knowledge requirement to find a copyright violation. Copyright infringement is a strict liability crime. When a work is copied, even if the person making the copy does not know, or have reason to know, that the work is copyrighted, an infringement may still be found.[235] Even subconscious copying has been held to be an infringement.[236]

One protection the Copyright Act gives to a computer information system is a compilation copyright. A compilation copyright gives the SYSOP a copyright on the data contained in the computer information system as a whole.[237] This does not give the SYSOP a copyright to the individual copyrighted elements carried on the system, but it does allow a copyright for the way the material is organized.[238] An example of this would be the electronic journal composed from articles submitted by users. The compiler of the journal would not own a copyright to the individual articles, but he or she would own a copyright in those elements which are original to the compiler, i.e., the selection and arrangement of the articles which makes up the periodical as a whole.[239] A bulletin board system could presumably also copyright its entire message base.

An exception to the exclusivity of a copyright is the "fair use" doctrine.[240] Section 107 of the Copyright Act[241] allows the use of portions of copyrighted material in another work without the need to secure permission of the copyright holder under certain circumstances. Such use is allowed, for example, "for purposes such as criticism, comment, news reporting, teaching . . . [or] scholarship or research."[242] There are limits, however, to what constitutes fair use and what constitutes copyright infringement. "[F]air use was traditionally a means of promoting educational and critical uses. Fair use, then, is an exception to the general rule that the public's interest in a large body of intellectual products coincides with the author's interest in exclusive control of his work, and it

234. *See* Screen Gems-Columbia Music, Inc. v. Mark-Fi Records, Inc., 256 F. Supp. 523 (S.D.N.Y. 1966).

235. De Acosta v. Brown, 146 F.2d 408 (2d Cir. 1944).

236. Bright Tunes Music Corp. v. Harrisongs Music, Ltd., 420 F. Supp. 177 (S.D.N.Y. 1976).

237. 17 U.S.C. § 103.

238. *Id.*

239. Feist Publications, Inc. v. Rural Tel. Serv. Co., No. 89-1909, 1991 U.S. LEXIS 1856 (S. Ct. Mar. 27, 1991).

240. 17 U.S.C. § 107.

241. *Id.*

242. *Id.*

is decided in each case as a matter of equity, using the four factors in the Act as guidelines."[243]

The first factor is whether the use is for a commercial, non-commercial or educational purpose.[244] The law favors non-commercial use over commercial use,[245] so that a SYSOP who pirates a competing service's material to lure away the other service's paying clients will more likely be guilty of an infringement than a SYSOP who quotes a competitor's material to illustrate what other services are available.

A SYSOP who uses copyrighted material for commercial uses faces two presumptions—first, that the use is not a fair use,[246] and second, that every commercial use poses a potential harm to the market for or value of the copyrighted work.[247]

The next issue a court addresses in determining whether a use is fair is the purpose of the original material.[248] Some works are more likely to be quoted or reviewed than others, and therefore excerpts of these works are less likely to be seen as infringements.

The third issue is how much and how important is the copied portion in relation to the whole?[249] The larger the percentage of the work copied, the more likely the work will be seen as an infringement.

Lastly, courts look to see how the copying affects the market for the original work.[250] A use of the copyrighted work which makes the original obsolete will obviously be more likely to be found an unfair use than a use which brings more notoriety to the original.

Another exception to the exclusivity of a copyright is found in section 108 of the Copyright Act.[251] Section 108 allows limited copying by libraries and archives. The section allows one copy to be to be made and/or distributed, as long as it is not done for commercial gain, the archive is open to the general public, and the copy contains a copyright notice.[252] Applying this section to computer information systems produces an interesting issue: it is easy for a computer archive to only contain one copy of a copyrighted work; however, it is possible for each viewer to retain a copy in the process of "viewing" the work. In fact, it is theoretically possible for an unlimited number of people to view the "single copy" simulta-

243. Note, *Digital Sound Sampling, Copyright and Publicity: Protecting Against the Electronic Appropriation of Sounds*, 87 COLUM. L. REV. 1723, 1736 (1987).

244. 17 U.S.C. § 107(1).

245. *See* Note, *supra* note 243.

246. Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1983).

247. *Id.*

248. 17 U.S.C. § 107(2).

249. *Id.* § 107(3).

250. *Id.* § 107(4).

251. *Id.* § 108.

252. *Id.*

neously. Paradoxes such as this have led people to believe that "the established canon of copyright and patent law is . . . fundamentally inadequate to the demands of the Information Age."[253]

2. *Copyrighted Materials on Computer Information Systems*

a. Copyrighted Text

Copyrighted text can appear on computer information systems as either files on a file server or database; or in an E-mail message or post on a BBS; or in an E-journal. The most obvious place to find copyrighted text is on information systems such as Lexis/Nexis, Westlaw and Dialog. Textual material, such as electronically stored journals, gets a fairly straightforward copyright analysis. The hardest job for a SYSOP may be discovering what text is copyrighted. Once infringing text is discovered, the SYSOP must remove it, or risk being held vicariously liable as a copyright infringer.[254]

b. Copyrighted Software

Bulletin board systems, network file servers, and mainframe computers that use FTP (File Transfer Protocol) all offer the opportunity to copy software. The Software Publisher's Association (SPA) offers the opportunity to be on the receiving end of a lawsuit if any of that copied software is copyrighted. The SPA is a trade association for software publishers. One of its goals is to reduced software piracy. The SPA monitors bulletin board systems for distribution of copyrighted software. They warn SYSOPs that they will be monitored, giving the SYSOP the opportunity to remove any software he or she does not have the right to distribute. The SPA also examines office computers for unlicensed software. Violators are asked to remove illegally held software, purchase legally licensed copies, and pay a fine equal to the amount of the purchase price of the software package. Compliance with the SPA requirements saves the offender the additional cost of a lawsuit.[255] Noncompliance will result in a lawsuit filed by the SPA.

As mentioned, not all copying of copyrighted software is illegal. Two exceptions are worth noting. One is making backup copies. The Copyright Act allows a copy of legally licensed software to be made if such a copy is needed to use the software.[256] The Act also allows a copy to be

253. Barlow, A Not So Brief History of the Electronic Frontier Foundation (available over Internet by anonymous FIP from FRP.EFF.ORG).

254. *See* Screen Gems-Columbia Music, Inc. v. Mark-Fi Records, Inc., 256 F. Supp. 523 (S.D.N.Y. 1966).

255. *See generally* Mason, *Crackdown on Software Pirates; Industry Watchdogs Renew Efforts to Curb Illegal Copying*, COMPUTERWORLD, Feb. 5, 1990, at 107.

256. 17 U.S.C. § 117(1).

made for archival purposes, as long as the copy is destroyed "in the event that continued possession of the computer program should cease to be rightful."[257]

The other exception is *shareware*. Shareware is a popular method of software publishing which allows a software programmer to distribute his or her work without all of the marketing costs, often via a computer information system.[258] A user can call up a BBS, download software, and try it out for a while. If the user likes the software, he or she sends the programmer a shareware fee. The difference between shareware and public domain software is that public domain software is freely distributed with the consent of the copyright owner, while shareware is not distributed without restriction—use of shareware beyond a reasonable trial period (often specific in the documentation distributed with the software) without payment of the shareware fee is a violation of copyright law.[259]

c. *Copyrighted Pictures*

As mentioned earlier,[260] pictures can be scanned into a computer and stored. Pictures can also be drawn directly on a computer by means of graphics software. A hybrid of the two is also possible—pictures can be scanned, and once scanned, can be further altered with image processing software.[261] All of these forms are covered by the Copyright Act.[262]

Pictures created on the computer using graphics or "paint box" software are an original copyrightable work of authorship.[263] Scanned images violate the original copyright holder's rights, unless permission to make the scanned image has been obtained,[264] even if no further distribution occurs.[265] As one author said, "[t]he law is quite straightforward; a copy is a copy, period. There is no wording that differentiates among images produced by scanners, by photocopiers, or by crocheting them into toilet seat covers."[266]

---

257. *Id.* § 117(2).

258. Givens, *Sharing Shareware: Non-Traditional Marketing Relies on Honor System*, ST. LOUIS BUS. J., July 1, 1991, § 2, at 1B.

259. *Id.*

260. Mason, *supra* note 255.

261. The legal aspects of doctoring photographs are beyond the scope of this paper. For a good discussion of such issues, see Seecof, *Scanning into the Future of Copyrightable Images: Computer-Based Image Processing Poses a Present Threat*, 5 HIGH TECH. L.J. 371 (1990).

262. 17 U.S.C. § 102(a)(6).

263. *Id.* § 102(a).

264. *Id.* § 101 (defining "copy); *id.* § 106 (the copyright holder has the exclusive right to make copies and derivative works of his or her creation).

265. *Id.* § 101.

266. Shapiro, *More on Copyright; Digitizing of Copyrighted Images*, MACWEEK, Oct. 11, 1988, at 27.

Non-copyrighted images such as those on which the copyright has already expired[267] can be scanned without violating the Copyright Act. Indeed, if sufficient creativity is contributed in the scanning process, the scanned images may be eligible for copyright protection in their own right.[268]

If a scan of a copyrighted picture is altered into a new image, the modified version may still fall under the original copyright.[269] It, therefore, would enjoy no protection on its own, and a copyright release would be required from the copyright holder to distribute the image (or to modify it in the first place).[270]

Once again, one of the most difficult tasks for a system operator is determining which images are copyrighted. The Copyright Act provides an author with the right to have his or her name associated with his or her own work, as well as the right to have his or her name disassociated with a mutilation of his or her work (along with the right to prevent such mutilations in the first place).[271] Based on these rights, a SYSOP should be especially careful of images which appear to be doctored.

Some of the larger computer information services allow the storage and distribution of images under the assumption that no one will mistake a scanned copy for an original, and therefore, there is no damages.[272] This argument has no basis in copyright law. The Copyright Act gives the author the exclusive right to make copies of his or her work, and this includes bad copies.[273]

Also, the claim that no damage is being done is an unreasonably narrow view. The copyright holder, and not the public, is allowed exclusive control of the channels through which his or her work reaches the market.[274] Computerized images present a whole new market for an artist's work, and widespread, unauthorized distribution can destroy the

267. 17 U.S.C. § 302 (applying to works created after Jan. 1, 1978, provides that a copyright shall expire fifty years after the death of the author).

268. *See, e.g.*, Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 63 (1984) (photographs are copyrightable by virtue of the creativity that goes into arranging the subject elements and photographic variables into a distinct picture).

269. 17 U.S.C. § 106. *See* Gracen v. Bradford Exchange, 698 F.2d 300 (7th Cir. 1983). *Cf.* Copyright Registration for Colorized Versions of Black and White Motion Pictures, 37 C.F.R. § 202 (1987).

270. 17 U.S.C. § 106A.

271. *Id.*

272. Shapiro, *Copywrongs on Consumer Info Networks? Posting of Scanned Images on Electronic Services Infringes Copyrights*, MACWEEK, Aug. 30, 1988, at 20.

273. 17 U.S.C. § 106.

274. Franklin Mint Corp. v. National Wildlife Art Exchange, 675 F.2d 62 (3d Cir. 1978). *See also* Zaccini v. Scripps-Howard Broadcasting Co., 433 U.S. 562 (1977) (TV station recorded and broadcast the plaintiff's entire act (human cannonball), depriving the plaintiff of a chance to sell tickets to the television viewers, since they had already seen his act).

potential to disseminate the work in the computer market—a right clearly given to the author of the work.

Some computer information services also raise the possibility that some of their stored images are provided on the basis of the "fair use"[275] exception.[276] Relying on fair use is not a very realistic position to take. One artist found some of his work scanned and available on a BBS after he was told of its presence by a friend. The artist's name and copyright notice had been cropped off. By the time the artist protested, 240 people had downloaded his images.[277] Such widespread infringement in a potentially new market for the artist's work is not likely to be found by a court to constitute "fair" use. For a SYSOP to be free from liability, the only thing he or she can do is to make sure the image is either not protected by copyright, or that the use of the image has been approved by the copyright holder.

The same analysis applies to sampled sounds stored in a computer information system; though for sounds it is even more difficult to determine what material is being distributed in violation of the copyright laws.

In addition, if there is a false attribution as to the origin of the work and an element of unfairness or deception, unauthorized use of copyrighted material on a computer information system may constitute unfair competition.[278] Unauthorized use where "a plaintiff believes that the defendant, at little or no cost, has appropriated what the plaintiff considers the plaintiff's own commercially valuable property" may constitute a subset of unfair competition—misappropriation.[279]

III. LIABILITY FOR COMPUTER INFORMATION SYSTEM CONTENT

To determine who is liable for illegal activity of the kind discussed thus far, it is necessary to know how computer information systems are viewed by the law. Computer information systems may be seen by the law as analogous to one of the other communications media, such as newspapers or common carriers, or they may be seen as a unique medium. Specific legislation geared towards the computer media has already been discussed. However, the law still leaves some issues unresolved. To resolve these issues, it is necessary to understand how

275. 17 U.S.C. § 107.

276. Shapiro, *supra* note 272.

277. Horton, *Electronic Ethics of Photography; Use of Images in Desktop Publishing*, FOLIO, Jan. 1990, at 71.

278. Note, *Original Digital: No More Free Samples*, 64 S. CAL. L. REV. 135, 163 (1990).

279. *Id.* at 165.

other media are regulated and how computer information systems are similar to or different from those media.

In all cases where the law would hold a party guilty for actions occurring on a computer information system, this article assumes that the SYSOP is liable if he or she is the initial cause of that violation because the law, by its terms, would clearly apply to the system operator. The primary question at issue here is the extent of a SYSOPs liability for illegal conduct conducted by the users of the computer information system.

A. Information System as Press

Many services on a computer information system are similar to those of print publishers. Just as there are magazines and newspapers, there are electronic periodicals. Just as there are street corner pamphleteers, so are there E-mail activists. Just as First Amendment privileges apply to the print media, so, one can argue, they should apply to the electronic press. Often the only practical difference between print media and electronic media is paper. In fact, with electronic word processing and page layout programs used by most print publishers, even printed periodicals at one stage exist in the same form as electronic journals.

Even bulletin board operators sometimes see themselves as being analogous to print publishers. Prodigy is an example of a service that sees itself as a publisher. In fact, Prodigy refers to the people who screen messages posted in their conferences as "editors" and not censors, and Prodigy claims all of them have journalism backgrounds.[280] Both Prodigy and the local newspaper take "articles" by "authors" and "publish" them in their respective media for the consumption of their "subscribers."

There are two types of publishers, primary and secondary. A *primary publisher* is presumed to play a part in the creative process of creating the message which is then disseminated.[281] Primary publishers are what one generally thinks of when thinking of publishers. Prodigy claims to be such a publisher. While the Constitution provides some protection to the editor's judgment as to what to print,[282] the protection is not complete. All of the restrictions on content discussed earlier apply to publishers—advocacy of lawless action, child pornography, obscenity,

280. Kapor, *A Day in the Life of Prodigy*, Effector Online, Vol. 1, No. 5 (Electronic Frontier Foundation, available over the Internet by anonymous FTP from FTP.EFF.ORG).

281. Charles, *Computer Bulletin Boards and Defamation: Who Should be Liable? Under What Standard?*, 2 J.L. & Technology 121, 131 (1987).

282. U.S. Const., amend. 1.

defamation, etc.[283] The SYSOP, as an electronic publisher, shares the same liability as a print publisher would—for example, the *New York Times*[284] "actual malice" standard for defamation, and a "knowing" standard as required by the statutes forbidding the transportation of material involved in child pornography.[285] The publisher is generally held to know what is being published because he or she has editorial control over the material that is published.

The question then becomes, is knowledge enough to result in liability? This is determined by the actual crime with which the publisher is charged. Defamation, for example, requires the publisher to have published the defamation with "knowing or reckless disregard for the truth."[286] For a SYSOP, at least a "know or have reason to know" standard would be necessary. A publisher generally knows he or she is publishing, as well as what is being published. A SYSOP for a large computer information system with a lot of users may not be able to keep track of all of the electronic journals and messages on bulletin boards which are being run on his or her system. While a SYSOP may have the same editorial control that a print publisher has, the sheer size may effectively prohibit actual editorial control over what is being published over the computer system. For this reason, it would be unfair to hold a SYSOP to a standard that requires less than a "know or reason to know" standard.

An argument for this minimum requirement is supported by some cases decisions. For example, there are decisions which hold that a publisher is not liable for everything in his or her periodical, such as the safety of products sold by their advertisers.[287] As the court in *Yuhas v. Mudge*[288] held:

> [t]o impose the [duty to check the truth of the claims of all of their advertisers] upon publishers of nationally circulated magazines, newspapers and other publications would not only be impractical and unrealistic, but would have a staggering adverse effect on the commercial world and our economic system. For the law to permit such exposure to those in the publishing business . . . would open the doors to 'liability in an indeterminate amount for an indeterminate time, to an indeterminate class.'

Operators of large systems are quick to support the view that the job of monitoring every communication on their systems would be a prohibi-

283. *See, e.g.*, § II.A. Defamation, § II.E Computer Crime.

284. New York Times v. United States, 403 U.S. 713 (1971).

285. 18 U.S.C. § 2252.

286. *New York Times*, 403 U.S. 713.

287. *See, e.g.*, Yuhas v. Mudge, 129 N.J. Super. 207, 209-10, 322 A.2d 824 (1974).

288. *Id.*

tively large task.[289] If a "know or have reason to know" standard were applied to computer information systems, offending material reported to a SYSOP would have to be dealt with under threat of liability. Also, any offending material discovered by the SYSOP would need to be removed. A SYSOP also could not avoid monitoring for improper content, knowing such content is present, and then later claim ignorance. However, holding a SYSOP responsible even for material that he or she did not know was on the computer system would require a much larger time commitment on the part of the SYSOP or the hiring of staff to supervise the activities taking place on the computer system. Most small hobbyists running bulleting board systems would not be able to support this additional commitment and would be forced to cease operating out of fear of liability. Larger commercial services would have to either increase costs to the users or decide that providing some services are no longer worth the expense. The net result would be a contraction of the number of outlets for free expression by means of computer.

By requiring at least a "reason to know" standard, a balance can be struck—the service can be provided, but a SYSOP could not hide his or her head in the sand to avoid liability. Any problem brought to the SYSOP's attention would have to be addressed; any problem the SYSOP discovered would also need to be taken care of; and any problem likely to be present could not be ignored by the SYSOP.

A *secondary publisher* is someone who is involved in the publication process, such as a press operator, mail carrier, or radio and television engineer, who usually does not know when a statement he or she transmits is defamatory and is usually not in a position to prevent the harm. A secondary publisher generally has no control over the content of the message, unlike a primary publisher.[290] Unless a secondary publisher knows or has reason to know of the defamatory nature of the material it is transmitting, it is free from liability for defamation.[291] Secondary publishers are often treated synonymously with republishers, who are discussed in the next section.

B. Information System as Republisher/Disseminator

A *republisher* or *disseminator* is defined as "someone who circulates, sells, or otherwise deals in the physical embodiment of the published material."[292] Some computer information systems are like republishers be-

289. *Information Policy, Computer Communications Networks Face Identity Crisis Over Their Legal Status*, Daily Rep. For Executives, Feb. 26, 1991, at A-6.

290. Thornton, *Symposium: Legal Issues in Electronic Publishing: 6. Libel*, 36 Fed. Com. L.J. 178, 179 (1984).

291. *See* Restatement (Second) of Torts § 581 (1989).

292. Jensen, *supra* note 7, at 3.

cause all they do is make available files, just like a bookseller or library makes texts available. A librarian cannot be expected to read every book in the library, just as the system operator of a service may not be able to read every text file stored on the computer system. File servers and data bases can be large enough to store complete texts of books and periodicals, as users of services such as Westlaw and Lexis/Nexis are well aware. Computer information systems can also contain massive quantities of software, Email and electronic journals, all stored ready for users to peruse like a library book.

One of the characteristics of secondary publishers is that they are "presumed, by definition, to be ignorant of the defamatory nature of the matter published or to be unable to modify the defamatory message in order to prevent the harm."[293] The case that first established the immunity from liability for distributors, breaking the common law tradition, was *Smith v. California*.[294] *Smith* involved a bookseller who was convicted of violating a statute that made it illegal to deal in obscene materials. The lower court held violators of the statute strictly liable. However, Justice Brennan held that a law which holds a bookseller strictly liable for the contents of the books he or she sells is unconstitutional. He stated his reasons as follows:

> For if the bookseller is criminally liable without knowledge of the comments . . . he will tend to restrict the books he sells to the ones he has inspected; and thus the State will have imposed a restriction upon the distribution of constitutionally protected as well as obscene literature. It has been well observed of a statute construed as dispensing with any requirement of scienter that: "Every bookseller would be placed under an obligation to make himself aware of the contents of every book in his shop. It would be unreasonable to demand so near an approach to omniscience." [citation omitted] And the bookseller's burden would become the public's burden . . . The bookseller's limitation in the amount of reading material with which he could familiarize himself, and his timidity in the face of absolute criminal liability, thus would tend to restrict the public's access to forms of the printed word which the State could not constitutionally suppress directly.[295]

While this case did not determine what degree of liability was appropriate for a bookseller, it did find that strict liability was inappropriate.[296] Later courts, however, were willing to set a minimum standard of liability, and that standard was set to a "know or have reason to know" standard.[297]

---

293. Charles, *supra* note 281, at 131.

294. 361 U.S. 147 (1959).

295. *Id.* at 153.

296. *Id.* at 155.

297. Sexton v. American News Co., 133 F. Supp. 591 (N.D. Fla. 1955). *Cf.* Manual Enterprises v. Day, 370 U.S. 478 (1962).

Secondary publishers are also not required to investigate the contents of the messages they are delivering in order to avoid liability.[298] Recently, a court has applied the *Smith*[299] analysis to computer information systems. *Cubby, Inc. v. CompuServe, Inc.*[300] is a major decision supporting the analogy of the computer information system as a republisher or disseminator of media. CompuServe was one of the first public computer information systems. It was founded in 1969 as a time-sharing system by H&R Block in order to make use of some of its surplus computer facilities.[301] CompuServe is now so large that it contracts out its editorial control of various discussion groups to other companies, who maintain the forum in accordance with CompuServe's general guidelines.[302] The groups maintaining the forums are similar to print publishers—they take articles submitted by users and publish them, exerting editorial control over the material where necessary. CompuServe works, in essence, like an electronic book store. CompuServe sells to its users the materials that the discussion groups publish.

In *Cubby*, one of the forums uploaded and made available an on-line publication which allegedly defamed the plaintiff. CompuServe had no opportunity to review the periodical's contents before it was made available to CompuServe's subscribers. District Judge Leisure held that since CompuServe had no editorial control over the periodical, and CompuServe did not know or have reason to know of the defamation contained in the periodical, CompuServe was in essence "an electronic, for-profit library."[303] Like a bookstore or library, CompuServe had the option to carry or not to carry the periodical, but once the decision was made CompuServe had no editorial control over the periodical. The court recognized the function of technology and admitted that a computer database is the functional equivalent to a news distributor or a public library, and therefore, so as not to impede the flow of information, the same "know or have reason to know" standard should apply.[304]

This holding has a number of profound implications for the law governing computer information systems. First, it establishes a clear determination of SYSOP liability: where the SYSOP does not exert editorial control, and does not know or have reason to know of the dissemination of offensive material, he or she cannot be held liable. This also implies that once a SYSOP is made aware, or has reason to believe, that the

298. Sexton, 133 F. Supp. at 593.

299. Smith v. California, 361 U.S. 950.

300. 776 F. Supp. 135 (S.D.N.Y. 1991).

301. Carlsen, *Wide Area Bulletin Boards Emerge as Method of Corporate Communications*, S.F. BUS. TIMES, Mar. 15, 1991, at 15.

302. *CompuServe*, 776 F. Supp. at 135.

303. *Id.* at 140.

304. *Id.*

computer system is being used for illegal purposes, he or she is obligated to remedy the situation under penalty of liability. It also implies that a SYSOP can reduce potential liability by avoiding awareness of message content on his or her system, limited by the "reason to know" element. A SYSOP could not, however, escape liability by sticking his or her head in the sand while knowing that the computer information system was likely being used for illicit purposes. The scope of this holding is arguably broad, especially since the court relied on an obscenity case to determine a defamation issue. This means that the same standard may now apply in both defamation and obscenity cases involving computer systems whose operators do not exert editorial control.[305]

C. Information System as Common Carrier

Network transmissions, E-mail, and some other features of a computer information systems such as "chat" features all work in a way similar to a common carrier. A common carrier is a service that

> is [of] a quasi-public character, which arises out of the undertaking 'to carry for all people indifferently. . . .' This does not mean that the particular services offered must practically be available to the entire public; a specialized carrier whose service is of possible use to only a fraction of the population may nonetheless be a common carrier if he [or she] holds himself [or herself] out to serve indifferently all potential users.[306]

Importantly, a computer information system need not be classified according to only one communications analogy—a system can act at times like a publisher, and at times like a common carrier. A service is defined as a common carrier when it acts as such based on the way it conducts its activities.[307]

Common carriers have generally been considered secondary publishers,[308] and as such, have traditionally functioned under a reduced standard of liability.[309] That standard is, once again, a "know or have reason to know" standard of liability.[310] This standard has been widely adopted and applied to the electronic communications media: from telegraph,[311]

---

305. *See Compuserve Case: A Step Forward in First Amendment Protection for Online Services*, Effector Online Vol. 2, No. 3, Jan. 7, 1992 (Electronic Frontier Foundation, available over the Internet by anonymous from FTP.EEF.ORG).

306. National Ass'n of Regulatory Util. Comm'rs v. F.C.C., 533 F.2d 601, 608 (1976).

307. *Id.* at 608.

308. *See, e.g.*, Von Meyersburg v. Western Union Tel. Co., 54 F. Supp. 100 (S.D. Fla. 1944); Mason v. Western Union Tel. Co., 52 Cal. App. 3d 429, 125 Cal. Rptr. 53 (1975).

309. Restatement (Second) of Torts § 612 (1989).

310. *Id.* § 581.

311. Von Meyersburg, 54 F. Supp. at 100; Western Union Telegraph Co. v. Lesesne, 182 F.2d 135 (4th Cir. 1950); O'Brien v. Western Union Telegraph Co., 113 F.2d 539 (1st Cir. 1940).

to telephone,[312] and even to options such as telephone answering services.[313]

There are a number of reasons for applying a knowing standard to a common carrier. One reason is efficiency. Service providers would not be able to do their job (transmitting) as well if they also had to monitor content.[314] Another reason is fairness. Common carrier operators are not trained in what is libelous and what is not, and, even if they were, they would have to make many decisions at a quick rate—not a fair burden to place on the common carrier.[315] And a third reason is privacy. By removing a need for common carriers to monitor the content of transmissions, the likelihood that transmissions will be held private increases.

A "know or have reason to know" standard makes a lot of sense for computer networks, as all of the above interests would be served by regulating a network as a common carrier. Like a common carrier, computer networks carry data from one computer to another with no regard for the information being transferred. Data transferred over a computer network often consists of electronic mail being forwarded from an account on a sending machine to an account on a receiving machine. Network traffic may also contain confidential documents being passed from computer to computer. Support for a "knowing" standard comes from the Electronic Communications Privacy Act of 1986,[316] which statutorily applies this standard to the interception and use of intercepted E-mail and network communications. For a SYSOP to be liable for a user's illegal use of the system, the SYSOP would have to know or have reason to know that the illegal use was going on, and he or she would then be under an obligation to prevent such a use.

It is worth mentioning at this point that not all communications over a common carrier are unregulated. There are some uses of electronic common carriers which are forbidden—an example is obscenity by telephone. A recent issue with the growth of 900 telephone numbers has been "dial-a-porn," where people can call a number and hear sexually-oriented messages. The use of a telephone to convey obscene, indecent, or harassing messages is outlawed.[317] An exception is made for indecent telephone messages, so long as provisions are used to prevent minors from receiving these indecent messages.[318] Allowable safeguards include: scrambling messages so they cannot be understood without a

312. Anderson v. New York Tel. Co., 35 N.Y.2d 746, 361 N.Y.S.2d 913, 320 N.E.2d 647 (App. 1974).

313. People v. Lauria, 251 Cal. App. 2d 471, 59 Cal. Rptr. 628 (1967).

314. Charles, *supra* note 281, at 143.

315. *Id.* at 123.

316. 18 U.S.C. § 2510 *et seq.*

317. 47 U.S.C. § 223.

318. 47 C.F.R. § 64.201.

descrambler; issuing a password by mail with age verification; or requiring a credit card number before transmission of the message.[319]

While this statute applies only to communication over a telephone, it does not distinguish between aural and data communications. Without making this distinction, the statute may also cover bulletin board systems or other services which provides indecent material. If this statute were applied to computer information systems, as it is applied to dial-a-porn, SYSOPs would have to employ one of the same means of preventing access to minors, and would have to make sure that the service offered met the standards of constitutionally protected indecency and that it did not cross the line into prohibited obscenity.[320]

As discussed earlier, there is no national standard for obscenity. A SYSOP would have to be careful not to break the obscenity laws in any state to which the computer information system reached. With the ease of access of a computer information system by means of a long distance telephone call, this would make computer information systems subject to the obscenity laws of every state. It is not hard to see how computer porn services should be subject to regulation in the same form as dial-a-porn. In both cases, the material being transmitted to the caller is the same: for dial-a-porn the material is transmitted aurally; for computer porn it is transmitted over a computer screen visually. With a computer's ability to transmit images and sounds as well as text, the justification for regulating computer distributed indecent material is equal to or great than the justification for regulating standard audio dial-a-porn.

The regulations on dial-a-porn could simply be applied in a computer context. The distribution means is essentially the same—a wire connection from the sender to the receiver. In the case of dial-a-porn, this wire is a telephone line. In the case of material transmitted by computer, the wire is either a telephone line or a network connection. The means of preventing access by minors could also be made the same, regardless of the means of access—a password, a credit card, or age verification by mail could still be required to access the service.

D. Information System as Traditional Mail

Since a major use for computer information systems is sending E-mail, it is only sensible to compare such a use to the U.S. mail. The U.S. mail is a type of common carrier mandated expressly by the Constitution.[321] U.S. mail, or "snail mail," is governed by a statute which gives

319. *Id.*

320. *See* Sable Com. v. F.C.C., 492 U.S. 116 (1989).

321. U.S. Const., art. I, § 8.

"regular" mail the same kind of privacy that the Electronic Communications Privacy Act[322] gives E-mail. The postal service act punishes:

> [w]hoever takes any letter . . . out of any post office or any authorized depository for mail matter, or from any mail carrier, or which has been in any post office or authorized depository, or in the custody of any letter or mail carrier, before it has been delivered to the person to whom it was directed, with design to obstruct correspondence, or prys into the business or secrets of another, or opens, secretes, embezzles, or destroys the same.[323]

This statute has the same effect as the statutes specifically geared towards electronic communications—it protects both mail in transmission,[324] as well as mail being stored for the recipient.[325] Just as the Electronic Communications Privacy Act protects stored communications in the form of an E-mail recipient's "mail box,"[326] so does the postal service protect a recipient's mail box.[327]

U.S. mail recipients have certain protections which E-mail recipients may also create for themselves. U.S. mail recipients can ask the post office to block mail from particular senders who are distributing what the receiver sees as sexually offensive mail.[328] However, the reason for this protection from unpleasant U.S. mail, which is based on notions of trespass,[329] could easily apply to E-mail and network communications as well. In the case of electronic mail, a computer program could be set up to automatically reject incoming mail from certain senders. A program could also be used to search through the text of an incoming message which contained certain terms which would indicate that the message's contents were something which the receiver did not want to see.

The same similarity analysis between E-mail and the U.S. Mail would work to preserve an advertiser's right to send out E-mail for commercial purposes, just as commercial U.S. mail enjoys some constitutional protection.[330] The one significant bar to the creation of a large junk E-mail industry is access. The U.S. mail is a true common carrier and as such they do not prohibit material based on advertising content. E-mail in many contexts may appear to be a common carrier, but if it is

---

322. *Supra* note 318.

323. 18 U.S.C. § 1702.

324. 18 U.S.C. § 1702, *compared to* E-mail, 18 U.S.C. § 2510.

325. 18 U.S.C. § 1702, *compared to* E-mail, 18 U.S.C. § 2511.

326. 18 U.S.C. § 2511.

327. *Id.* § 1702; *see also* United States Postal Serv. v. Council of Greenburgh Civic Ass'n, 453 U.S. 114 (1981).

328. Rowan v. United States Postal Dept., 397 U.S. 728 (1970).

329. *Id.* at 737.

330. Bolger v. Young Drug Prods. Corp., 463 U.S. 60 (1983).

sent over a company's computer system, for instance, there may be no way for an advertiser to gain access to the company's E-mail system.

Similarly, large networks such as the Internet exist for educational purposes. While network authorities do not censor E-mail, in keeping the network in line with the definition of a common carrier, a user could still report a company which was trying to advertise over the network. Since the Internet is not meant to be used for profit making purposes, an offending company reported by a user could be denied access privileges to the network.

E. Information System as Traditional Bulletin Board

For centuries courts have been looking at liability for notices posted on bulletin boards, bathroom walls, sides of buildings, and wherever else defamatory material can be posted. In the past few hundred years there has been little debate about proprietor liability for the content of the "bulletin boards" under its control. The law of Great Britain, as parent to the U.S. legal system, is illustrative. The English Star Chamber in *Halliwood's Case*[331] held that "if one finds a libel, and would keep himself out of danger, if it be composed against a private man, the finder may either burn it or deliver it to a magistrate."

A fairly modern case (1937) cited more frequently in this country is *Byrne v. Deane*.[332] This case involved a poem, placed on the wall of a private golf club, which was alleged to be defamatory[333] of one of the club's members. Hilbery, J., held that the owners of the club could be held liable as republishers of the defamation. He based this conclusion on the fact that the club owners had complete control of the walls of the club; they had seen the poem; they could have removed it; and yet they did not. In the words of Greer, L.J., "[B]y allowing the defamatory statement . . . to rest upon their wall and not to remove it, with the knowledge that they must have had that by not removing it it would be read by people to whom it would convey such meaning as it had, were taking part in the publication of it."[334]

Courts in this country have made rulings on the posting of defamatory material since at least 1883. *Woodling v. Knickerbocker*[335] involved two placards left on a table at a furniture dealer, one which read, "[t]his was taken from Dr. Woodling as he would not pay for it; for sale at a bargain," and the other which read, "Moral: Beware of dead-beats." The

331. *As quoted in* Byrne v. Deane, 1 K.B. 818, 824 (1937).

332. *Byrne*, 1 K.B. at 818.

333. The court held against the plaintiff on the grounds that the message was not defamatory.

334. *Byrne*, 1 K.B. at 830.

335. 31 Minn. 268, 17 N.W. 387 (1883).

court found for the plaintiff, holding that regardless of who left the sign, anyone who allowed or encouraged its placement, or who had authority to remove the sign after it was placed, could be held liable for its publication. Importantly, the court also discussed the liability of one of the furniture store owners who had not seen the defamation. The court said that she could not be held liable for her partner's nonfeasance in removing the sign because there was no way to imply that she had given him authority to act as a publisher of defamatory material, and this was beyond the scope their business.[336]

This situation was contrasted with that of a business involved in publishing or selling books or magazines.[337] In the case of a publisher or seller, all of the partners are to be regarded as having given authority to the other partners in deciding what to publish or sell, and therefore all of the partners are to be held liable for defamation. This implies that a SYSOP who either does not monitor the content of publicly accessible parts of the system under his or her control, or a SYSOP or computer information system owner who delegates such responsibility may still be held liable for defamatory material.

Fogg v. Boston & L. Railway Co.[338] supports this theory. In this case, a newspaper article defaming a ticket broker was posted in the defendant's railway office. The court held that a jury could properly have found that the defendant, by way of its agents, had knowledge of what was posted in its office.[339] Also, by not removing it in a timely manner the company could be construed as having endorsed or ratified the posting of the defamatory article, even if it had not been responsible for its posting in the first place.

Hellar v. Bianco[340] is a case where the proprietor of an establishment was originally unaware of the defamation, and this case raised the issue as to what constituted a reasonable time to remove defamatory posts once a proprietor is made aware of their existence. *Hellar* involved "libelous matter indicating that appellant was an unchaste woman who indulged in illicit amatory ventures"[341] which was scrawled on a men's room wall of a tavern. After the woman who was the subject of the note began getting calls about the graffiti, the bartender was asked to have the message removed. Later that evening, when it was not removed, the tavern owner was charged with republication of the libel. The court held that republication occurred when the bartender knew of the libel, and

336. *Id.*
337. *Id.*
338. 20 N.E. 109 (Mass. 1889).
339. *Id.*
340. 244 P.2d 757 (Cal. App. 1952).
341. *Id.* at 758.

had an opportunity to remove it, but did not do so.[342] Under these circumstances, a short period of time was sufficient to constitute republication.

A longer period of time was found not to constitute republication in *Tacket v. General Motors Corp.*[343] *Tacket* involved a defamatory sign posted in a GM factory. The court said that it was conceivable that it could take three days to remove a sign because of the speed at which large bureaucracies work. The court did say that a second sign which had been posted for seven or eight months was different and that a lengthy time of posting without removal could be found by a jury to be republication by implied ratification.

A more recent case, *Scott v. Hull*[344] appears, at first glance, to hold in a manner contrary to these earlier cases. In *Scott*, graffiti defaming the plaintiff was written on the side of a building. The plaintiff told the defendant about the graffiti and asked that it be removed; the defendant refused. The court held that the building owners were not liable as republishers and they were under no duty to remove the graffiti. The reasoning behind this decision is that the viewing of the graffiti was not at the invitation of the owners—as it was in the earlier cases.

In *Scott*, the graffiti was on the outside of the defendant's building. It was placed there by strangers and read by strangers. The defamation was not put there by an act of the defendant, and the court refused to find liability for nonfeasance in this instance. In *Hellar*,[345] the defamation was "published" in the restroom on the defendant's premises. The graffiti was placed there by invitees of the defendant, and was read by other invitees. *Byrne*,[346] *Woodling*[347] and *Tacket*[348] are similar to *Hellar*. The same was true in *Fogg*,[349] except there the defamation was even related to the defendant's business.

Invitee analysis of defamation raises two issues involving computer information systems. First, can someone post "outside" of a computer? An example of this might be someone who defames someone by electronic mail sent from one user on a computer to several others. If the injured party sued the operator of a bulletin board which also runs on that computer, the invitee analysis would indicate that the BBS operator could not be held liable. This would make sense assuming the BBS SYSOP has nothing to do with the electronic mail, *and* has no control over the

342. *Id.*
343. 836 F.2d 1042 (7th Cir. 1987).
344. 269 N.E. 160 (Ohio App. 1970).
345. *Hellar*, 244 P.2d at 757.
346. *Byrne*, 1 K.B. at 818.
347. *Woodling*, 31 Minn. at 268, 17 N.W. at 387.
348. *Tacket*, 836 F.2d at 1042.
349. *Fogg*, 20 N.E. at 109.

mail system. Although the offending message is on the same computer as the bulletin board system, the mail does not appear on the computer at the request of the BBS operator, unlike a post left by a user invited to use the BBS. Messages sent by E-mail would go beyond the scope of the BBS's invitation; therefore it would be unreasonable to hold the bulletin board operator liable responsibility would fall on the operator of the mail system.

If, however, the BBS operator had been given the power to remove an offending message left anywhere on the computer system, then an agency argument would say that the BBS SYSOP has the duty to remove the offending message, or have someone else do it. This is similar to the case of graffiti in a bar—a bartender could not easily claim immunity from a defamation charge with the argument that removing graffiti was not the job of a the bartender. If the bartender was not hired to clean, the bartender could at least inform someone who was, rather than leave the defamatory graffiti in place.

The second issue the invitee analysis raises is messages posted by someone who is clearly not an invitee—for instance, a computer hacker who is essentially a trespasser. In this situation, a SYSOP should likely be required to remove any defamatory messages left by a hacker under the same reasoning as the above cited cases.[350] These cases all assume that the writing was left by an invitee, so just because defamatory messages are left by a trespasser does not mean the SYSOP or building owner should be any less liable if they know of the message, have the opportunity to remove it, and yet do not do so.

F. Information System as Broadcaster

With the rise of packet radio and radio WANS (wireless networks), the analogy of a computer information system as broadcaster is also of growing importance. Authority to govern broadcasting is given to the F.C.C. under the Communications Act of 1934.[351] The justification for content regulation over the airwaves is "spectrum scarcity"—there are only so many radio and television stations that can be on the air at once. "Without government control, the medium would be of little use because of the cacophony of competing voices, none of which could be clearly and predictably heard."[352] In order to preserve the "market place of ideas" from monopolization, the F.C.C. governs the use of the airwaves to preserve the rights of viewers and listeners to be informed.[353] An equal concern is to protect children from inappropriate material; this is espe-

350. *Supra* notes 331-49.
351. 47 U.S.C. § 301 *et seq.*
352. Red Lion Broadcasting Co. v. F.C.C., 395 U.S. 367, 376 (1969).
353. *Id.* at 390.

cially true because of radio and television's special reach—it can even bring indecent messages to those children too young to read.[354] Radio and television are given special treatment, including the "channeling" of constitutionally protected speech, because:

> 1. children have access to radios and in many cases are unsupervised by parents; 2. radio receivers are in the home, a place where people's privacy interest is entitled to extra deference; 3. unconsenting adults may tune in a station without any warning that offensive language is being or will be broadcast; and 4. there is a scarcity of spectrum space, the use of which the government must therefore license in the public interest.[355]

These reasons allow the F.C.C. to promulgate rules to channel constitutionally protected "indecent" speech to times of the day when children are not as likely to be in the listening audience, but the F.C.C. may not altogether prohibit indecent speech.[356]

The four factors justifying channeling of speech do not work very well when applied to wired computer communication, such as computer information systems. No spectrum scarcity issue is involved when calling a computer information system. Any indecent material available via computer must be actively sought, as there is no risk of having the telephone ring and being assaulted by a computer spewing lewd data. While computers, like radio receivers, are in the home, it takes an active effort to obtain indecent material via computer, so the risks of accidental exposure to such material at issue in the broadcasting situation are just not present.

Finally, although children do have unsupervised access to computers, they also may have some potential unsupervised access to dial-a-porn and cable television. Neither dial-a-porn nor cable are restricted as severely as broadcasting. As far as the four factors justifying channeling of indecent speech applying to wireless data transmission (packet radio, radio-WAN), the element of spectrum scarcity comes back into play, giving the F.C.C. more of a reason to regulate computer communications sent via the airwaves. However, it is less likely that offensive material will accidentally be received, since data being broadcast may be encrypted in order to avoid its unauthorized interception by minors.

As well as channeling indecent speech, the other exceptions and guarantees of free speech that apply to publishers apply to broadcasters.[357] For instance, a broadcaster does not have the right to make defamatory statements with knowing or reckless disregard for the truth.[358]

---

354. F.C.C. v. Pacifica Foundation, Inc., 438 U.S. 726 (1978).
355. *Id.* at 731.
356. Action for Children's Television v. F.C.C., 932 F.2d 1504 (D.C. Cir. 1991).
357. *See supra* § II.A Defamation; II.E Computer Crime.
358. Adams v. Frontier Broadcasting Co., 555 P.2d 556 (Wyo. 1976).

Cable television and cable audio signals are governed in a similar fashion to regular broadcasting. These services are seen as an "ancillary" services to broadcasting, and therefore fall under the F.C.C.'s authority.[359] Like computer information services, but unlike broadcasting, cable television must be actively brought into the home. Because of this, cable television traditionally was not seen as being as "pervasive" as broadcasting, and therefore the *Pacifica*[360] obscenity standard traditionally was not extended to cable.[361]

Recent cable television regulation, however, acknowledges the growth of cable, which now reaches nearly sixty per cent of all television households.[362] The Communications Act of 1934[363] allowed a cable franchising authority to prohibit or restrict any service that "in the judgement of the franchising authority is obscene, or is in conflict with community standards in that it is lewd, lascivious, filthy, or indecent or is otherwise unprotected by the Constitution of the United States." The 1992 amendments to the Communications Act allow a cable operator to establish a policy of excluding "programming that the cable operator reasonably believes describes or depicts sexual or excretory activities or organs in a patently offensive manner as measured by contemporary community standards."[364] Thus, this standard taken from *Pacifica* now can be applied to cable television. The new amendments require the F.C.C. to create regulations to channel indecent material onto a single cable channel which must then be blocked out unless requested in writing by the subscriber, thus preventing access by minors.[365] Also, analogous to the postal service statutes, the new cable regulations add a provision for service users to have the service provider block out unsolicited sexually explicit materials on request.[366]

Because wired computer networks are more like cable, cable provides a better analogy than broadcasting. In fact, as mentioned earlier,[367] teletext services are usually provided over cable television. The use of computers over the air waves is currently limited, but it promises to increase in the future as technology advances. In any case, because computer data can be easily encrypted, radio networks do not share the

359. 47 U.S.C. § 151 *et seq.*; *see also* United States v. Midwest Video Corp., 406 U.S. 649 (1972).

360. *Pacifica*, 438 U.S. at 726.

361. Community Television, Inc. v. Roy City, 555 F. Supp. 1164 (D. Utah 1982); Cruz v. Ferre, 755 F.2d 1415 (11th Cir. 1985).

362. Cable Television Consumer Protection and Competition Act of 1992, Pub. L. No. 102-385, § 2(3), 106 Stat. 1460, Oct. 5, 1992.

363. 47 U.S.C. § 532(h).

364. Cable Television Consumer Protection Act of 1992, § 10(a)(2).

365. *Id.* at § 10(b).

366. *Id.* at § 15.

367. *See supra* § I.A.2 Teletext and Videotex or Videotext.

same need for content restrictions that broadcasters require. While cable television is a better analogy for traditional computer information services than is broadcasting, some of the other regulatory schemes still fit computer information systems more tightly. This is because computer information systems do not provide the same sorts of services as cable television. Rather, computers are used as the common carriers, bulletin boards, and electronic presses that have already been discussed.

IV. SUGGESTIONS FOR REGULATION

Now that the current regulatory environment of computer information systems has been discussed, one is left wondering how well the regulations function to control Cyberspace. Many people fear that the current law does not effectively protect the rights of voyagers through Cyberspace. This has given rise to groups such as Computer Professionals for Social Responsibility[368] and the Electronic Frontier Foundation.[369] Groups such as these work to increase access to technology for the general masses; to help legislatures understand what it is they are regulating; to help aid in the passing of responsible, workable laws; and, where necessary, to help defend people whose rights are being violated because of legislation which does not properly cover computer information systems.

Constitutional law professor Laurence Tribe has even proposed a new amendment to the Constitution to protect individuals from such violations of their rights. His proposed amendment reads:

> This Constitution's protections for the freedoms of speech, press, petition, and assembly, and its protections 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.[370]

This amendment would serve to ensure that the speech and privacy right that we currently enjoy in other media would be applied to electronic communications as well. An amendment such as this would avoid incidences like the Operation Sun Devil raid on Steve Jackson Games.[371] This amendment would serve to guarantee that a computer bulletin

368. Ring, *Computer Professionals for Social Responsibility Seeks to Change Lay Preconceptions*, COMPUGRAM INT'L, Oct. 9, 1990.

369. Barlow, *Crime and Puzzlement: In Advance of the Law on the Electronic Frontier; Cyberspace*, WHOLE EARTH REV., Sept. 22, 1990, at 44.

370. Laurence Tribe Proposed Constitutional Amendment, (document on file with the Electronic Frontier Foundation, available over Internet by anonymous FTP from FTP.EFF.ORG).

371. *See* § II.E. Computer Crime.

board publishing the contemporary editor's message would enjoy the same constitutional protection as the print publisher's printing press.

Some authors focus more on how liability should be assessed and damages determined in a new medium which offers the opportunity for violation of rights on an instantaneous, global scale. For example, one author[372] believes that SYSOPs should be at least jointly liable with the poster of the offending material. He argues that the average subscriber to a BBS does not have the resources to compensate adequately for injuries caused by the potentially widespread reach of offending material. Also, it may not even be able to discover the reach of offending material. Copyrighted material could be spread from computer to computer all over the world after just one file transfer.

Others want to simplify the issue of system operator liability by holding the SYSOP liable, in addition to the original poster, as a means of compensating victims and deterring misuse.[373] These people argue that SYSOPs should be liable for content because they are easier to track down than the users who posted the offending material, and also, by holding them liable, SYSOPs are more likely to work at deterring others from the use of their service for inappropriate purposes.

What is necessary to regulate computer information system content and system operator liability is, first and foremost, an understanding of the technology. The law is a slow evolving, tradition-bound beast. Computers are an upstart technology pioneered by people who do things like create viruses to let loose on their friends in order to hone their programming skills.[374]

If judges, juries, lawyers and legislators do not understand current technology, the technology will have changed before the law catches up to it. Many of our current laws will work well if adapted to computer information systems. The Electronic Communications Privacy Act of 1986[375] works well to regulate electronic mail because it is modeled after the statute that governs the U.S. mail.[376] For many people, these new communications fora are direct replacements for the ones that they represent; therefore they should be regulated like the ones they represent. This may entail using several different regulatory schemes, but this should not be too hard to employ by people who understand the technology at issue simply regulate E-mail like U.S. mail, regulate networks like common carriers, etc. It would not be difficult to employ the correct

372. Charles, *supra* note 281.

373. Gilbert, *Computer Bulletin Board Operator Liability for User Misuse*, 54 FORDHAM L. REV. 439, 441 (1985).

374. *See* Branscomb, *supra* note 137.

375. 18 U.S.C. § 2511.

376. *Id.* § 1702.

legal analogy if the computer information service at issue is looked at from the point of view of the user.

Where novel legislation is needed is in defining terms to be used in the developing law. An example is trespassing. If someone hacks into a computer system, is he or she breaking and entering, or is the situation more analogous to someone making a prank telephone call?

Tribe's proposed Constitutional amendment[377] is similar to a modern day spelling out of a natural law concept. The law already exists, so it should be assumed that the Constitution covers all technologies equally, including Cyberspace. In theory an amendment to the Constitution is not necessary; however, a new amendment would leave no doubts and would make for streamlined judicial decisions. As computer information systems grow in popularity and scope, older media will pass away. The structure already exists to regulate the new technology, because, in essence, the new technology is just a new incarnation of the old.

377. *See supra* text accompanying note 370.

GLOSSARY

Access To make use of a computer system, often from a remote location by means of a telephone or computer network.

Account Most computer users have an "account" which basically amounts to a name recognized by the computer (or "user ID" sometimes written just as "userid"), a password which allows access to the computer, and a set of "account privileges," which determine what the user can do with the account. Examples of account privileges may include electronic mail, storage space for data, and access to a network which allows the user to tap into remote computers' resources.

Backup To copy data stored on a magnetic computer disk or tape. The term also refers to the copy.

BBS Bulletin Board System. A BBS is a program which runs on a computer and allows people to call the BBS from their own computers or terminals. The program may offer any of a number of services. Typically, a BBS will provide a message area which allows a person calling up (called a user) to leave messages regarding a specific topic and read other messages left by other users on that topic. BBSs may be devoted to one specific topic, or they may have message areas for the discussion of several hundred topics. Many BBSs also have facilities for sending electronic mail. Electronic mail is similar in this case to a message posted in the regular topic areas, but appears only in another user's private "mailbox." Many bulletin board systems also offer files, consisting of either text or other computer software and the like, for users to "download" (transfer to their own computer). Some BBSs are available by telephone line, some over a computer network, some by both. Some BBSs allow only one user to use it at a time, some allow up to 50 or more simultaneously.

Bit-mapped Bit mapping, as it relates to fonts or typefaces, refers to a process of forming the image of a letter or character by calculating where to draw each dot (or "pixel") that composes the letter. The other major form of drawing letters is PostScript, which describes the shape of a letter as a series of lines and curves.

Bug Computer jargon meaning malfunction, generally in computer software or hardware.

Bulletin Board System *See* BBS.

CD-ROM Compact Disc-Read Only Memory. This is an optical form of data stored on a 5-inch plastic disc. Data is then read off of a disc with a laser, identically to the more familiar audio compact disc. CD-ROMs allow tremendous amounts of storage in a compact, durable form.

Chat A feature on many bulletin board systems that support multiple users simultaneously. A chat feature allows a user to send messages in-

stantaneously, or nearly so, to another user who is using the BBS at the same time.

Common Carrier A common carrier, in the media context, is a service provider who promises to carry its subscribers messages without discriminating on the basis of message content. The most familiar example of a common carrier is the telephone company.

Communications Provider A company which provides a service for transmitting messages from one of the service's users to another (or even the service provider itself to another user). This could be one user to one user, as in the case of the telephone company, or it could be one user to many users, as in the case of a broadcaster.

CompuServe One of the oldest and largest computer information systems, originally started by H&R Block to make use of some of its unused computer resources.

Computer An electronic device for processing information at extremely high speeds.

Computer Crime Any of a number of kinds of crime which are either caused by the use of a computer, or crimes against computers or computer data itself.

Computer Information System Any number of specialized computer services which provide various types of data to the computer's users. Data may consist of text, software, computerized pictures and sounds, or a means of communication between other computer users.

Computer Memory The part of a computer which stores information for the computer to process. This may consist of "RAM" (random access memory) in which a computer stores data which is needed either immediately or frequently, or it may consist of disk or tape storage which is used for storing less frequently needed data, or data which is too voluminous for the computer's RAM.

Computer Service A service provided through the use of a computer such as delivery of communications, storage of data, processing of information, etc.

Crash When a computer or part of a computer system stops functioning, due to some sort of malfunction, resulting in a loss of service.

Cyberspace A term coined by the science fiction author William Gibson for territory inhabited by electronic signals. This territory consists of the computer and telephone networks which connect together everything from telephones to automatic teller machines to interactive cable television. In some ways it is intangible, yet in other ways it is a "place" wherein people can communicate with others, do their work, and go to find means of entertainment.

Data Computer information of any kind.

Decoder A means of taking an encrypted signal which is otherwise unintelligible and altering it so it can be understood.

Descrambling *See* Decoder.

Dial-a-porn Sexually explicit discussions of sexual activity or situations obtainable over the telephone, generally charged for by calling a "900" number or by calling and giving a credit card number. Dial-a-porn has been the subject of quite a bit of legal controversy, and generates tremendous revenues for the service providers and for the telephone companies.

DIALOG A large computer information system which provides a wide variety of information from a wide variety of sources to the subscribers to the service.

Digital Of or pertaining to computer data. Digital information is composed of only zeros and ones (on or off, positive or negative) which when properly interpreted by a computer can be used to represent many different kinds of information. Digital data can be stored magnetically or optically, sent over a wire or even broadcast.

Digitizing The process of taking something and reducing it to a computer readable form, often used in the process of taking a picture and reproducing it in a form which can be manipulated by computer. See "Scanning."

Direct Dial A means of accessing a computer by means of a telephone line.

Disk A storage medium for storing computer data in a magnetic form.

Download The process of moving computer files from a "host" computer to a remote personal computer or another mainframe.

EFF Electronic Frontier Foundation. An organization founded by Mitch Kapor, creator of the Lotus 1-2-3 spreadsheet program, and John Perry Barlow, lyricist for the Grateful Dead. The organization's goals are to make computer resources available to everyone, not just an "information elite," to help pass responsible computer and information legislation, and to help protect the civil rights of computer users who are at the mercy of a legal system which often doesn't understand the issues and complexities of modern computer technologies.

Electronic Database A computer information system used to store tremendous amounts of information. Users can then give the database "search terms" which tell the computer to find any of the stored information that meets the user's criteria.

Electronic Communication Messages sent from a user on one computer to a user on another computer, or between two users on the same computer. An example of an electronic communication is an E-mail message.

Electronic Digest A form of electronic communication consisting of messages which are compiled and edited and then distributed to subscribers to the digest.

Electronic Forum A form of electronic communication. A forum consists of a group of people who send messages to all the other members of the group. A forum member sends a message to a "LISTSERVER" which automatically sends the message to all the other people on the LISTSERVER's electronic mailing list. Message recipients can then respond to the original sender, and all the other people who have received the original message in the same manner.

Electronic Frontier Foundation *See* EFF.

Electronic Journal Another electronic communication form. An electronic journal (or Ejournal) is similar to a print journal, except that it is distributed electronically to people's electronic mailboxes.

Electronic Mail Another form of electronic communication. Electronic mail, more often referred to simply as "E-mail" are messages that one computer sends to another by means of a computer. E-mail can be sent from one user to another using the same computer, or mail can be sent to users on different computers that are connected by a computer network. E-mail is particularly attractive to frequent computer users because it provides nearly instantaneous communication. Over a large computer network messages can be sent to the other side of the globe, often in s little as a few minutes.

Electronic Mailbox The portion of a computer user's account which stores electronic mail the user has received.

Electronic Publishing The process of producing messages, usually meaning larger electronic journals, which are then distributed to computer users by means of electronic mail instead of traditional "paper mail."

E-Journal *See* Electronic Journal.

E-Mail *See* Electronic Mail.

File A "chunk" of computer data, generally stored on a disk or tape. Files may be software, textual information, or even pictures or sounds.

File Server A computer information system designed to distribute files.

File System Part of a bulletin board system designed to operate as a file server.

File Transfer Protocol More commonly referred to as FTP. FTP is a means of transferring files from one computer connected to a network to another computer on that network at fast speeds. Often computers on major networks are set up to distribute files to anyone who wants them. This is accomplished without the necessity of having an account on the

host computer by a process known as "anonymous FTP." A number of documents used in writing this paper were acquired by anonymous FTP. To obtain such a document, all that is needed is as an account on a computer on the same network as the computer that has the desired file. You also need the network "address" of the computer the file is on, and you need to know what file you are looking for (and possibly where to look on the computer that has the desired file). Both computers must also be able to use the file transfer protocol.

Font *See* Typeface.

FTP *See* File Transfer Protocol.

Hacker Originally this term meant a person particularly adept at using a computer; now the term is often used to label someone who breaks into computer systems without authorization.

Host Computer A computer which a remote computer user is connecting to, generally either by means of a terminal or a personal computer acting as a terminal.

Image Processing Manipulating a picture by computer. Through the use of computer graphics software, an image can be altered or enhanced-picture elements can be re-arranged, colors and intensities can be altered, etc.

Information Distribution System A computer system which distributes data to its users, generally as some form of text.

Information Screen A "page" of computer data. If a computer is displaying text, the amount of information that will fit on the computer screen at any one time is sometimes called an information screen.

Information Service A computer service which is used to distribute data, usually some form of text.

Internet A "network of networks." The Internet is a network which connects many smaller regional or national computer networks, creating one large global computer network. The network is established to connect computers together which are used for research purposes. Computers connected to the Internet are from many of the world's colleges and universities, governments, and some businesses or other organizations.

LEXIS A computer information system which stores and distributes legal texts to subscribers who call the service with their computers.

Listserver A type of automated mailing list. A user can send a message to a Listserver instead of to another user's account. The Listserver then takes the message, and automatically mails copies of the message it has received to all of the people on its mailing list. The recipients can then respond in the same fashion.

Mainframe A large computer which generally supports a number of people sharing its resources at the same time.

Messages As referred to here, a form of electronic communication. Messages may either be E-mail, some sort of electronic digest or journal, or a message which can be sent directly from one user to another user who is using the same computer at the same time (such as a "chat" message).

Michaelangelo A recent, and particularly destructive, computer virus recently made popular by the media. It is named after the painter due to the fact that it is designed to trigger each year on the artist's birthday.

Minitel The French nationally sponsored computer information system.

Modem A device used to connect two computers to each other over telephone lines. Modem stands for modulator/demodulator. It functions by taking computer data, translating it into an audio signal and then sending it over the telephone line. A receiving modem then translates the signal coming over the wire back into computer data.

Morris, Robert Jr. The designer of the "Internet worm," a virus-like program which caused a number of computers on the Internet network to become "congested" and crash. this resulted in the first major case to apply the Computer Fraud and Abuse Act of 1986. This case also resulted in a profound expansion of the reach of that act.

Net Sex Similar to Dial-a-porn, but consisting of sending sexually explicit messages to users of a computer system, rather than between people using the telephone.

Network A number of computers which are connected together, allowing the computers to exchange data. Data can be anything from E-mail, to files, to commands from one user who is trying to make use of another computer's processing power.

News Server A computer information system which is designed to circulate a form of electronic mail between other computers, or different users on one computer.

One-Way Service A service which distributes data to users who request information, but which is incapable of handling any data the user desires to send back to the service.

Operating System Special computer software which controls machine functions. Operating systems run in the background behind any other software and serve as a sort of interpreter between the machine and the user. DOS is a kind of operating system used on an IBM. System 7 is a kind of operating software used on a Macintosh.

Operation Sundevil A major government operation which attempted to arrest perpetrators of computer crimes. Operation Sundevil seized in

the area of 40 computers and thousands of computer disks. It has been widely criticized as being abusive, overly-intrusive, uninformed, largely unsuccessful, and as having paid no attention to its targets' civil rights.

Packet Radio A means of sending computer data by means of amateur radio.

Password A set of letters or symbols used to provide security for a computer account. Anyone who tries to use a computer account must know the proper letters or symbols to gain access to that account. In an ideal world, a password will only be known by people authorized to use the account, and the computer's system operator.

Personal Computer A small, inexpensive computer generally owned by an individual, as opposed to a large mainframe costing many thousands of dollars.

Pixel Pixel stands for picture element. A pixel is a dot, which when looked at in relation to other pixels around it form a picture. For an example, take a close look with a magnifying glass at either a television screen or a newspaper photo.

Post To send a message for display on a publicly accessible area of a computer information system.

Postscript A way of drawing letters or symbols on a computer by use a series of lines and curves, as opposed to bitmapping which defines a letter or symbol by the location of a series of dots.

Processor The part of a computer which actually performs calculations.

Prodigy A major computer information system, formed as a joint venture between IBM and Sears.

Public Domain In this context it refers to computer software which is made available for anyone to copy without charge.

Radio-WANS Radio-Wide Area Network. This is a new technology which allows the transmission of computer data by radio waves. In essence it is a wireless computer network.

RAM RAM is a volatile information store where the computer keeps the information it is actively processing. When the computer is turned off, all of this data is lost.

Sampling The process of converting an audio signal to computer data. When a sound is sampled, a "snapshot" is taken of the sound; actually several thousand snapshots per second. The snapshot (also referred to as a sample) is then measured and assigned a value. The sound can then be represented by a succession of numbers which can be stored like any other computer data, and later reconstructed into a close approximation of the original sound. This is the same process at work with compact discs.

Scanning Pictures are put into a computer by a process called "scanning" or "digitizing." Scanning is accomplished by dividing a picture up into little tiny elements called pixels. The equivalent can be seen by looking very closely at a television screen or at a photograph printed in a newspaper. The computer then examines each of these dots, or pixels, and measures its brightness; the computer does this with each pixel. The picture is then represented by a series of numbers that correspond to the brightness and location of each pixel. These numbers can be stored as a computer file, and later reconstructed.

Scrambling Taking data and encoding it so it cannot be readily understood by those who do not know how to decode it.

Screen Refers to either a computer monitor, or display, or to as much information as can appear on the display at any one time.

Search Term A term used to search through an electronic database. For example, if you are searching through a card catalog in a library, you may use as a search term the author's name of the book you are trying to find, the book's title, the subject, etc. The actual name you are trying to find is the search term.

Server A computer system or account which operates to distribute data to anyone who requests it. This could be a file server which stores files for distribution over a network, or a news server which distributes news articles, a list server which works as an automated mailing list, etc.

Shareware Computer software that is freely distributed with the expectation (hope?) that people who receive copies of the software and decide to use it will send in a shareware fee to the author of the software.

Snail Mail The U.S. mail in computer jargon. It is referred to snail mail because the postal service is so much slower than electronic mail.

Software Sets of computer instructions which make the computer do some operation. These operations can be anything from playing a game to acting as a terminal to connect to another computer, helping you write a law review article, etc. Analogous to how a recipe instructs a chef as to how to bake a cake.

System Failure A problem with a computer system causing anything from temporary loss of service to permanent loss of information.

System Operator The person who is in charge of running a particular computer system or computer service. Generally the System operator has complete power over the system, he or she can read any file or data on or passing through the system, private or not, and he or she can erase any data or files found on the system. The System Operator generally also controls who has access to various parts of the system, and under what conditions.

SYSOP *See* System Operator.

Time bomb A type of computer virus which waits for a certain time or set of events to happen before triggering.

Teletext A type of computer information system. Teletext is a one-way service which can only distribute information to users, and does not know how to handle any sort of input from its users. Teletext services are often provided over cable television. It sends out a constantly repeating set of information over the television cable. A viewer selects what information he or she would like to see, and the next time the desired information is sent over the cable it is displayed on the television screen.

Terminal A computer device which is used to send commands and data to another computer. Terminals may be "dumb" terminals which can only send information to another computer for processing and have no processing power of their own. Or they can be "smart" terminals which are fully functioning computers themselves that can be used as terminals to connect to other computers. An example of a smart terminal would be a personal computer which has software which allows it to operate as a terminal.

Trap and Trace Device A device that can be attached to a telephone line to trace and record what phone number calls originated from that are made to the telephone line that is being monitored.

Trojan Horse A type of computer virus which hides inside other, generally innocuous, programs as a means of moving from one computer system to another.

Two-Way Service A service which allows people using the service to not only receive information, but send information back to the service as well.

Typeface A set of letters and symbols all sharing a characteristic look. Also referred to as a "font."

UNIX A computer "operating system" popular with larger, and many networked computers. UNIX provides the actual instructions on how a computer is supposed to operate, similar to DOS (disk operating system) on an IBM, or the Finder or System Software on a Macintosh.

Upload Process of transferring data from a personal computer to a "host" computer. Opposite of "download."

User Computer jargon for a person who uses a computer information system.

Videotex A computer service which transmits data over (generally) a telephone line. Videotex is a two-way service, allowing not only the service to send data to its subscribers, but also for the subscribers to send data back to the service.

Videotext *See* Videotex.

Virus A computer program which is used to annoy or cause harm to a computer or data used by the computer. There are many types of viruses. Some are "innocuous" while others can debilitate a computer system. Generally they are self replicating, and are transferred from computer to computer either over a computer network, or by infecting disks which are then used in other machines. There is a good deal of debate as to the actual definition of a virus.

WAN Wide Area Network. A type of network used to connect computers.

WESTLAW A computer information system which stores and distributes legal texts to subscribers who connect to the service with their computers.

Wiretap A device put on a telephone line used to listen to and/or record the contents of any telephone calls made over that telephone line.

Word Processor (also known as a "text processor") A computer program used to assist in the writing and editing of text. A finished docllment can be saved as a "text file" or "word processor file" or it can be used to edit messages to be sent by electronic mail.

Worm A type of computer virus (though considered by some not to be a true virus) which crawls from machine to machine, often used to search for and report information back to its creator. Information may be for a beneficial purpose, such as finding machines which are not being used to their full potential, or information may be for a more harmful purpose, such as finding weaknesses in computer security for use by hackers.