This paper first appeared in the Albany Law Journal of Science and Technology, Volume 3, Number 1. Care has been taken so that each printed page in this PostScript file corresponds to the same page in the printed volume, this way the paper may be cited without the need to track down an official printed copy.

David Loundy
465 Pleasant Ave.
Highland Park, IL 60035

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 electronically 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 paper, 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 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 paper 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. We will begin by looking at different types of computer information systems, and then the major legal issues surrounding

---

[1] Mitchell Kapor & John P. Barlow, *Across the Electronic Frontier*, July 10, 1990, *available over*

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 the analogy the courts decide to apply. Finally, an evaluation will be made of where the law affecting computer information systems now stands, and how it should be developed.

II. COMPUTER INFORMATION SYSTEMS DEFINED

A. *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 like. 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 connected to the host computer, a user can read the notes (also referred to as

---

Internet, by anonymous FTP, at FTP.EFF.ORG (Electronic Frontier Foundation).

[2] Each of the legal issues could be discussed in papers 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 beginning with 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. In addition to the computer, bulletin board software is also needed, which is obtainable either commercially or free. Finally, you need a way for people (usually called "users" in computer jargon) to access your bulletin board. This is accomplished via a modem or by 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. More and more often computers may be found connected together in a network, such as computers in a lab at a university, or office computers which share resources.

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 which means they can only be used by one person at a time. But some bulletin boards are able to support many users at the same time, 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.[7]

There are a number of different things bulletin board systems allow one to do. As their name implies, their primary function 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 availability of pornographic material, defamation, etc.

Another use for bulletin board systems is the sending of electronic mail, or E-Mail, as it is commonly called. Electronic mail

---

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

[7] Because of the way a BBS is accessed, some easily have national or international reach. The international aspects of computer information systems are beyond the scope of this paper, though 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 may be used by people in their home countries.

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 Eric C. 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 populace not just for local users, but also for users all over the world. Some countries already provide their citizens easy access to state-endorsed computer information systems. The world leader has been France, which has provided its "Minitel" service since 1982. Wallys W. Conhaim, *Maturing French Videotext becomes Key International Business Tool*, 9 INFO. TODAY 28 (1992). Minitel has grown to a system of about six million terminals as of the end of 1991, and it includes access to over 16,000 information services. Carol Wilson, *The Myths and Magic of Minitel; France s Minitel Videotex Service*, TELEPHONY, Dec. 2, 1991, at 52, 52.

is a message that is sent from one computer user to another, occurring 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.[8] 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.[9] 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."

Another service many bulletin board systems make available is 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. This 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]

---

[8] Robert W. Kastenmeier et al., *Communications Privacy: A Legislative Perspective*, 1989 WIS. L. REV. 715, 727.

[9] *Id.*

[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, solely based on the messages they have exchanged. John Johnston, *Looking for Log-On Love*, Gannett News Service, Mar. 25, 1992, *available in* LEXIS, Nexis Library, Currnt 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 20 percent of the usage of its conferencing system. John Markoff, *The Nation; The Latest Technology Fuels the Oldest of Drives*, N.Y. TIMES, Mar. 22, 1992, § 4, at 5.

B. *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.[15] It sends out a continually repeating set of information screens.[16] By using a decoder, a user can select which screen he or she wants.[17] The decoder then "grabs" the requested screen and displays it as it cycles by.[18] 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[19] (often called videotext).[20] Videotex is a two-way service which usually uses a personal computer as a terminal.[21] When provided via a telephone, videotex is basically the same as any other computer information system discussed in this paper, so the terms "videotex" and "computer information system" are used synonymously for ease of discussion.

C. *Information Distribution Systems*

Computers are used frequently for distributing information of various types. One common type of information distribution system is the database.[22] These services allow the user to enter a variety of "search terms" to look through the information the service has collected.[23]

Another type of information distribution system is the "file

---

[14] *See generally* Richard N. Neustadt, *Symposium: Legal Issues in Electronic Publishing: 1. Background -- The Technology*, 36 FED. COM L.J. 149 (1984).

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] 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 [hereinafter Glossary].

[21] Neustadt, *supra* note 14, at 149.

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

[23] Some of these services are quite large, and may contain the whole text of books and periodicals, though 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.

server."[24] A file server (or just "server") is a storage device, such as a disk drive or CD ROM, hooked up to a computer network, which lets any computer connected to it access the files contained on the server.[25] These files may 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.[26]

D. *Networks*

A network is a series of computers, connected often by special types of telephone wires.[27] Many networks are conduits used to call up a remote computer in order to make use of that computer's resources from a remote personal computer or terminal.[28] Many networks allow a much broader range of uses such as sending E-mail and more interactive forms of communication between machines,[29] transferring computer files, and also providing the same remote access and use that the simpler networks allow.[30]

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.[31]

---

[24] *See* MACUSER, June 1991, at 134.

[25] *See Glossary, supra* note 20.

[26] On large networks, such as the Internet, there are even databases called "archies," which index file servers available all over the network. They have small descriptions of available software, and give a listing of what machines on the network have the file available. Alan Emtage, *What Is Archie*, EFFECTOR ONLINE, Oct. 18, 1991, *available over* Internet, by anonymous FTP, at FTP.EFF.ORG (Electronic Frontier Foundation)(Vol. 1, No. 12).

[27] CHRISTOPHER CONDON & YALE COMPUTER CENTER, BITNET USERHELP, 1988. Available over Bitnet by sending the command "get bitnet userhelp" to NETSERV@BITNIC. *Id.*

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

[29] 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.

[30] Some examples of these more full-service type networks include the Internet, Bitnet, and ARPANET.

[31] One such special use is the electronic forum, basically an automated mailing list. A message is sent to a "LISTSERVER" where it is then 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; the LISTSERVER then 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, which includes 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

E. *Issues Involved*

Computer information systems present a whole slew 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? Is it the user who originally posted the defamation, or the system operator who controls and provides the forum? Currently, these are hotly debated issues.

Whenever a new communications medium develops, there is a risk that 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.

One major use for computer information systems is transferring files; in fact, that is the whole purpose for services such as file servers. Legal issues arise when these transfers contain copyrighted material for example, either text, pictures, sounds, or computer software which violates copyright law.

A growing threat to computer users is the computer virus. The Computer Virus Industry Association reports that in 1988, nearly 90,000 personal computers were affected by computer viruses.[32] 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.[33]

Privacy is another issue for users and system operators of

---

discussion if they do not log on to read their mail regularly. CONDON & YALE COMPUTER CENTER, *supra*, note 27. A similar type of electronic publication is the electronic digest; 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 E-journal. These are "real" magazines, just like print magazines, but they are distributed electronically, rather than in hard copy. *Id.*

[32] Dawn Stover, *Viruses, Worms, Trojans, and Bombs; Computer Infections*, POPULAR SCI., Sept. 1989, at 59.

[33] *Id.* Some people consider them such a threat that Lloyd's of London even offers an insurance policy that specifically covers viruses. *Id.*

computer information systems. 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."[34] Yet, how does this Amendment apply to Cyberspace. 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 arise 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 they provide out of fear of liability.

F. *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."[35] Many publishers use BBSs to supplement their printed editions either by providing additional stories or by providing computer information services on a BBS.[36] 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 similarity exists because computer services can be provided by sending data over the airwaves, thus providing the same services available from computers networked together by wire. Computer services can also be used to

---

[34] U.S. CONST. amend. IV.

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

[36] *See generally Fred The Computer ; Electronic Newspaper Services Seen as Ad-Ons*, COMM. DAILY, Apr. 10, 1990, at 4.

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 that 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.

III. CURRENT REGULATORY ENVIRONMENT

The current regulatory environment governing computer information systems is somewhat confused because of the multiplicity of the 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, computer information systems are not regulated by the F.C.C.[37] 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."

---

[37] Second Computer Inquiry 61 F.C.C.2d 103 (1976) (Amendment of Section 64.702 of the Commission's Rules and Regulations, Notice of Inquiry and Proposed Rulemaking). *See also* Second Computer Inquiry, 77 F.C.C.2d 384, 420-21 (1980) (Final Decision) (The talks directly discuss BBSs as enhanced services.).

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 one post there is potentially defamatory speech, speech advocating lawless action, fighting words, and an admission and solicitation of child pornography.

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; E-mail can contain defamatory statements. Defamation can even be distributed in the form of a scanned photograph.[38] But what is defamation, and what risks and obligations does it present to a system operator?

Defamation occurs in two forms — 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

---

[38] See Gregory G. Sarno, Annotation, *Libel and Slander: Defamation by Photograph*, 52 A.L.R. 4th 488, 495 (1987).

form and "no respectable authority has ever attempted to justify the distinction on principle."[39] 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.[40] 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 judges used the generic term "defamation."[41]

Slander is publication in a transitory form — speech, for example, is slander.[42] 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 characteristic of written or printed words."[43] 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 also last longer, 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.[44] 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 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 pre-meditated 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

---

[39] RESTATEMENT (SECOND) OF TORTS § 568 cmt. b (1989).

[40] *Id.*

[41] *See, e.g.*, Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc. 472 U.S. 749 (1985).

[42] RESTATEMENT (SECOND) OF TORTS § 568(2).

[43] *Id.* § 568(1).

[44] *See* Tidmore v. Mills, 32 So. 2d 769, 774 (Ala. Ct. App.), *cert. denied*, 32 So. 2d 782 (Ala. 1947).

and unprivileged statement to a third person.[45] "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]."[46] 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 refusal to deal with the object of the statement; rather the words used must merely be likely to have such an effect.[47] 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.[48] "Community" does not refer to the entire community, but rather to a "substantial and respectable minority" of the community.[49] Even more specifically, the community is not necessarily seen as the community at large, but rather as the "relevant" community.[50] 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 don't know whether Sam's accusations of child beating are true. If they are, Sam would have a defense against a charge of libel. The comment is being "published" to any other BBS user who reads the message Sam has left publicly, and as already discussed, the computer message has the same harmful qualities as a message written 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

---

[45] RESTATEMENT (SECOND) OF TORTS § 558 (1989).

[46] *Id.* § 559.

[47] *Id.* § 559 cmt. d.

[48] *Id.*

[49] *Id.* § 569 cmt. e.

[50] *See, e.g.*, Ben-Oliel v. Press Publishing Co., 167 N.E. 432 (N.Y. 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.

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 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 left unprotected. Analysis is based on the party or parties privy to the defamation. In our hypothetical, the relevant parties are Sam and Dora. Constitutional protection was first found for some types of defamation in *New York Times v. Sullivan*.[51] This case involved an advertisement taken out in a newspaper expressing grievances with the treatment of blacks in Alabama.[52] An elected city commissioner sued, claiming that the statements made in the advertisement defamed him and that the advertisement contained some inaccuracies.[53] Justice Brennan argued that the case should be considered "against the background

---

[51] New York Times v. Sullivan, 376 U.S. 254 (1964).

[52] *Id.* at 256.

[53] *Id.*

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."[54] The court held 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.[55] Because of this, the court said libel laws should be relaxed where the speech pertains to the affairs of elected officials.[56] Likewise, due to the importance of being able to examine the worthiness of public officials, the court felt that speech critical of officials should also be less open to attack on grounds of falsity.[57] 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.[58] 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.[59] A balance between open debate and freedom from defamation was struck by establishing an "actual malice" standard of liability for the publisher.[60] "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.[61]

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

---

[54] Id. at 270.
[55] Id. at 279.
[56] Id.
[57] Id.
[58] Id.
[59] Id.
[60] Id. at 279-80.
[61] Id.

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 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 Slammer's statement may be privileged, presuming no actual malice was intended.

The *New York Times* standard was expanded in two important cases, *Curtis Publishing Co. v. Butts*,[62] and its companion case, *Associated Press v. Walker*.[63] Both cases involved defamation of people who did not fit under the "public official" heading, but who were "public figures." As discussed in the concurrence, some people, even though they are not part of the government, are nonetheless sufficiently influential to affect matters of important public concern.[64] The Court subsequently has 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 ... ."[65] Because these people have influence in our governance, just as public officials do, the same "actual malice" standard should apply to such public figures.[66] Here, as in the case of public officials, we don't really 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.*[67] In *Gertz*, a magazine published an article accusing a lawyer of being a "Communist-fronter" and a "Marxist."[68] The article accused the plaintiff of plotting

---

[62] Curtis Publishing Co. v. Butts, 388 U.S. 130 (1967), *aff g* 351 F.2d 702 (5th Cir. 1965), *reh g denied*, 389 U.S. 889 (1967).

[63] Associated Press v. Walker, 388 U.S. 130 (1967), *rev g* 393 S.W.2d 671 (Tex. Civ. App. 1965), *reh g denied*, 389 U.S. 889 (1967).

[64] *See* 388 U.S. at 164 (Warren, C.J., concurring).

[65] Gertz v. Robert Welch, Inc., 418 U.S. 323, 342 (1974). *See infra* text accompanying notes 67-79.

[66] 418 U.S. at 343.

[67] *Id.* at 323.

[68] *Id.*

against the police.[69] The plaintiff was a lawyer who played a role in the trial of a police officer who was charged with shooting a boy.[70] The lawyer sued for defamation. The publisher's defense was based on another exception to defamation law that the court had carved out in *Rosenbloom v. Metromedia, Inc.*[71] *Rosenbloom* extended the *New York Times* standard to include not just public officials and public figures, but also private figures who were actively involved in matters of public concern.[72] The *Gertz* court held that this expansion went too far,[73] and the court overruled *Rosenbloom*.[74] The court in *Gertz* acknowledged that the press should not be held strictly liable for false factual assertions where matters of public interest were concerned.[75] Strict liability would serve to chill the publisher's speech by leading to self censorship where facts are in doubt.[76] This First Amendment interest was balanced against the individual's interest in being compensated for defamatory falsehood.[77] The court reasoned that private individuals were deserving of more protection than public officials and public figures because private persons do not have the same access to channels of communication, and they have not voluntarily exposed themselves to the public spotlight.[78] 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."[79] Courts have not made it very difficult for private people to sue for defamation where there is no matter of public concern at issue; in one of the more famous defamation cases, *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*,[80] Dun & Bradstreet was held liable for a credit report made from inaccurate records contained in a database.[81] The court argued that statements on

---

[69] Id. at 326.

[70] Id.

[71] See Rosenbloom v. Metromedia, Inc., 403 U.S. 29 (1971).

[72] Id. at 31-32.

[73] 418 U.S. at 345.

[74] Id. at 346.

[75] Id. at 340.

[76] Id.

[77] Id. at 341.

[78] Id. at 344.

[79] Id. at 347.

[80] 472 U.S. at 749 (involving a suit for defamation because of a false credit report).

[81] Id.; cf. Thompson v. San Antonio Retail Merchants Ass'n, 682 F.2d. 509 (5th Cir. 1982).

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.[82]

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 people's inabilities to pay their debts can be a matter of public concern, as was found in the *Dun & Bradstreet* case,[83] 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 as a result of the kind of news the press is reporting. One such privilege, is for fair report, or "neutral reportage,"[84] (which is not an issue in our hypothetical). This isolates a reporter from defamatory statements that he or she is reporting.[85] The reasoning behind this is that the fact that some statements were made is a matter of public interest, especially around sensitive issues, and therefore the public interest is best served by allowing the press to inform people of these statements without the risk of liability.[86] 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 therefore the fair report privilege will not apply.

Statements of opinion are also privileged.[87] Protection of opinion is, of necessity, not absolute otherwise "a writer could escape liability ... simply by using, explicitly or implicitly, the words 'I think.'"[88] Sam Slammer cannot defend himself by saying, "Well, I think Dora beats her daughter." The court in *Cianci v. New Times*

---

[82] 472 U.S. at 761-62.

[83] *Id.*

[84] *See*, Edwards v. National Audubon Soc'y, Inc., 556 F.2d 113 (2d. Cir. 1977). *See also* Time, Inc. v. Pape, 401 U.S. 279, *reh'g denied*, 401 U.S. 1015 (1971) (Newspaper's coverage of a government report 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) (holding a publisher that exactly reprinted a court opinion was absolutely privileged for any defamatory comments in the court opinion).

[85] 763 F.2d at 68.

[86] 556 F.2d at 119.

[87] *See, e.g.*, Greenbelt Coop. Publishing Ass'n v. Bresler, 398 U.S. 6 (1970).

[88] Cianci v. New York Times Publishing Co., 636 F.2d 54, 64 (1980).

Publishing Co.[89] succinctly laid out the limits of the opinion privilege:

> (1) that a pejorative 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.[90]

In the hypothetical, Sam made an outright accusation that Dora Defamed committed 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.

In sum, what this means for computer information systems, whether speech on a bulletin board, text in an electronic journal, or in any of the other forms of electronic publication, is that liability may result if the message is libelous. It may 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 if it lowers the opinion of the user 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."[91] The First Amendment is one of the most important guarantees in the Bill of Rights, because speech is essential for securing other rights.[92]

---

[89] *Id.*

[90] *Id.* (referring to Greenbelt Coop. Letter Carriers v. Austin, 418 U.S. 264 (1974); Gertz v. Robert Welsh 418 U.S. 323 (1974); Buckley v. Littell, 539 F2d 882, *cert. denied*, 429 U.S. 1062 (1977); Rinaldi v. Holt, Rinehart & Winston, Inc., 366 N.E.2d 1299 (N.Y.), *cert. denied*, 434 U.S. 969 (1977)) (The court in Cianci held the privilege inapplicable to a situation in which the plaintiff was clearly accused of committing a criminal act.).

[91] U.S. CONST. amend. I.

[92] *Legal Overview: The Electronic Frontier and the Bill of Rights*, *available over Internet*, by anonymous FTP, at FTP.EFF.ORG (Electronic Frontier Foundation).

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, although it is, at times, more restrictive.[93] An example of such a restriction is the regulation of radio and television by the Federal Communications Commission.[94] 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,[95] 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.[96] 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*.[97] The court in *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 of law violation "where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action."[98] Sam threatened to kill Dora, and he urged others to kill her as well. An important distinction is made between mere advocacy and incitement to imminent lawless action —the first is protected speech, 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 have been posted. It is hard to imagine such "stale" messages as advocating *imminent* lawless action. In our hypothetical, Sam encourages anyone near

---

[93] *Id.*

[94] Hereinafter F.C.C.

[95] Matt Kramer, *Wireless Communication Net: Dream Come True; Wireless Distributed Area Networks The Wide View*, P.C. WEEK, Mar. 5, 1990, at 51, 51.

[96] Harvey Silverglate, *Legal Overview, The Electronic Frontier and the Bill of Rights,available over* Internet, by anonymous FTP, at FTP.EFF.ORG (Electronic Frontier Foundation).

[97] Brandenburg v. Ohio, 395 U.S. 444 (1969).

[98] *Id.* at 447.

the computer Dora is using to go 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, for example, 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.[99] In *Chaplinsky v. State of 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."[100] 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.[101] 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* as there is in *Brandenburg*.[102] Fighting words can be considered delivered to the addressee when the message is read. Dora will become enraged when she reads Sam's message. When Sam left the message has little bearing on when Dora will be ready to fight. 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

---

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

[100] *Id.*

[101] *Id.* at 573.

[102] *Compare id. with* 395 U.S. at 446.

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 which he was word processing is suddenly missing from his computer account.

D. *Child Pornography*

Other areas of content are regulated on computer information systems. One is child pornography. *New York v. Ferber*[103] 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.[104] Second, application of the *Miller* standard for obscenity (discussed *infra*) is not a satisfactory solution to the problem of child pornography.[105] 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.[106] Fourth, the value of permitting minors to perform/appear in lewd exhibitions is negligible at best.[107] Finally, classifying child pornography as a form of expression outside the protection of the First Amendment is not incompatible with earlier court decisions.[108] The court said, "[T]he distribution of photographs and films depicting sexual activity by juveniles is intrinsically related to the sexual abuse of children ..."[109] 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.[110] Section 2252 of Title 18 of the U.S. Code forbids knowing foreign or interstate transportation or reception by any means

---

[103] New York v. Ferber, 458 U.S. 747 (1982).

[104] *Id.* at 756-57 (citing Globe Newspaper Co. v. Superior Court, 457 U.S. 596, 607 (1982)).

[105] *Id.* at 759 (citing Miller v. California, 413 U.S. 15, *reh'g denied*, 414 U.S. 881 (1973)).

[106] *Id.* at 761.

[107] *Id.* at 762.

[108] *Id.* at 763.

[109] *Id.* at 759.

[110] *See* 18 U.S.C. § 2252 (1978).

including, for example, visual depictions of minors engaged in sexually explicit conduct which have been converted into a computer-readable form.[111]

Pictures are easily converted into a computer-readable form. Once in such a form, they can be distributed, interstate, over a computer information system. Pictures are put into a computer by a process called "scanning" or "digitizing."[112] Scanning is accomplished by dividing a picture up into little tiny elements called pixels.[113] 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.[114]

Computers 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 prosecuted for child abuse, and such a suit could result in $50,000 or more in fines and damages.[115] 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 prosecution for child abuse.

Another issue raised by section 2252 is possession of pornographic material. Anyone who "knowingly possesses 3 or more books, magazines, periodicals, films, video tapes, or other matter which contain 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

---

[111] *Id.* § 2252(a)(1).

[112] *See* Lois F. Lunin, *An Overview of Electronic Image Information*, OPTICAL INFO. SYSS., May 1990.

[113] *Id.*

[114] *Id.*

[115] *See* 18 U.S.C. § 2255(a) (1986).

have been mailed or so shipped or transported, by means including computer"[116] can be fined and imprisoned for up to five years.[117] While the requirement of knowledge may insulate some computer information syrems 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 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 which was 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 Sam 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 may be considered to have constructive knowledge of the presence of the pornographic material on her system, and therefore she could be charged 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

---

[116] § 2252(a)(4)(B).

[117] *Id.* § 2252(b).

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.[118] Law enforcement use of bulletin board systems to track down pedophiles has not resulted in prosecutions of system operators, but there have been convictions of BBS users who have arranged to make "snuff films" through contacts they have made over a computer.[119]

E. *Computer Crime*

Some areas of "computer crime" are regulated.[120] Computer crime is an issue which computer information system operators should be aware of, as they may be on the receiving end at some point. The term "computer crime" covers a number of offenses,[121] such as: the unauthorized accessing of a computer system;[122] the unauthorized accessing of a computer to gain certain kinds of information (such as defense information or financial records);[123] accessing a computer and removing, damaging, or preventing access to data without authorization;[124] trafficking in stolen computer passwords;[125] spreading computer viruses;[126] and a number of other related offenses.[127] All of these are activities which are often referred to as "hacking."[128]

---

[118] *See*, Jim Doyle, *FBI Probing Child Porn On Computers: Fremont Man Complains of Illicit Mail*, SAN FRANCISCO CHRON., Dec. 5, 1991 at A23. *See also*, Robert F. 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.; Robert L. Jackson, *Child Molesters Use Electronic Networks; Computer-Crime Sleuths Go Undercover*, L.A. TIMES, Oct. 1, 1989, at 20.

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

[120] Note, *Addressing the New Hazards of the High Technology Workplace*, 104 HARV. L. REV. 1898, 1913 (1991).

[121] *Id.* at 1898.

[122] *See* 949 F.2d 133; Jensen, *supra* note 7, at 222.

[123] *See* 949 F.2d 133; Note, *supra* note 120, at 1898; Jensen, *supra* note 7, at 222.

[124] *See* 949 F.2d 133; Note, *supra* note 120, at 1898; Jensen *supra* note 7, at 222.

[125] Note, *supra* note 120, at 1899; Jensen, *supra* note 7, at 222.

[126] *See* United States v. Morris, 928 F.2d 505 (2d Cir.), *cert. denied*, 112 S. Ct. 72 (1991).

[127] Jensen, *supra* note 7, at 222.

[128] *Id.*

F. Computer Fraud

The first federal computer crime law, entitled the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, was passed in October of 1984.[129]

> [T]he Act made it a felony knowingly to access a computer without authorization, or in excess of authorization, in order to obtain classified United States defense or foreign relations information with the intent or reason to believe that such information would be used to harm the United States or to advantage a foreign nation.[130]

Access to obtain information from financial records of a financial institution or in a consumer file of a credit reporting agency was also outlawed.[131] 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.[132] The 1984 Act had several shortcomings, and was revised in The Computer Fraud and Abuse Act of 1986.[133] The 1986 Act added three new crimes — a computer fraud offense,[134] modeled after federal mail and wire fraud statutes;[135] an offense for the alteration, damage or destruction of information contained in a "federal interest computer;"[136] and an offense for trafficking in computer passwords under some circumstances.[137]

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.[138] Robert T. Morris Jr. was charged with releasing a "worm" onto a section of the Internet computer network,[139] causing numerous government and university computers to either

---

[129] Dodd S. Griffith, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 455 (1990).

[130] *Id.* at 460.

[131] *Id.*

[132] *Id.*

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

[134] Griffith, *supra* note 129, at 474.

[135] *Id.*

[136] *Id.*

[137] *Id.*

[138] United States v. Morris, 928 F.2d 504 (2d Cir.), *cert. denied*, 112 S. Ct. 72 (1991).

[139] *Id.*; Nicholas Martin, *Revenge of the Nerds; The Real Problem with Computer Viruses Isn t Genius Programmers, It s Careless Ones*, PSYCHOL. TODAY, Jan. 1989, at 21.

"crash" or become "catatonic."[140] Morris is the son of the Chief Scientist at the National Security Agency's National Computer Security Center.[141] His father is also a former researcher at AT&T's Bell Laboratories where he worked on the original UNIX operating system.[142] UNIX is the operating system that many mainframe computers use. Morris claims that the purpose of his worm program was to demonstrate security defects and the inadequacies of network security, not to cause harm.[143] However, due to a small error in his worm 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.[144] 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 ....[145]

Judge Munson's interpretation is that this language requires intent only to access the computer, not intent to cause actual damage.[146] On appeal, Munson's reading was affirmed by the Court of Appeals,[147] and the Supreme Court refused to hear further appeals.[148]

Morris' lawyer, Thomas Guidoboni, described the statute as "perilously vague" because it treats intruders who do not cause any harm just as severely as computer terrorists.[149] 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.

---

[140] 928 F.2d. at 506.

[141] Robin Nelson, *Viruses, Pests, and Politics: State of the Art*, 20 COMPUTER & COMM. DECISIONS, Dec. 1989, at 40, 40.

[142] Id.

[143] 928 F.2d. at 504.

[144] Id. at 506.

[145] 18 U.S.C. § 1030(a)(5)(A).

[146] 928 F.2d at 506-07.

[147] 328 F2d. 504 (1991).

[148] 112 S. Ct. at 72.

[149] Thomas A. 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, 33.

criminal justice system, which almost always differentiates between people who intend to cause harm and those who do not.[150] No one seems to argue that what Morris did was *right*, but many do not agree that he should be charged with a felony although he was convicted.[151]

The jury in the Morris case indicated that the most difficult question was whether Morris' access to the Internet was unauthorized even though defense counsel pointed out that 2 million subscribers had the same access.[152] The jury's difficulty in resolving this issue is indicative of a lack of understanding of how computer networks work.[153]

G. *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.[154] They can also break into telephone companies' computers and get lists of telephone credit card numbers.[155] Trafficking of stolen credit card numbers and other kinds of telecommunications fraud costs long distance carriers about $1.2 billion annually.[156] 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.[157] The major protection for the telephone companies is found in section 1343 of the Mail Fraud Chapter of the U.S. Code.[158] This section prohibits the use of wires, radio or television in order to fraudulently deprive a party of money or

---

[150] *Id.*

[151] Mike Godwin, *Editorial: Amendments Would Undue Damage of Morris Decision*, EFFECTOR ONLINE, Oct. 18, 1991, *available over Internet*, by anonymous FTP, at FTP.EFF.ORG (Electronic Frontier Foundation).

[152] David F. Geneson, *Recent Developments in the Investigation and Prosecution of Computer Crime*, 301 PLI/Pat 45, at 2. The difficulty arises from the fact that Morris had authorized access to some computers but not others, presenting the question whether Morris' actions amounted to unauthorized access or whether his actions exceeded authorized access. 928 F.2d at 510.

[153] Geneson, *supra* note 152, at 2.

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

[155] *Id.*

[156] *Id.*

[157] *Id.*

[158] Fraud by Wire, Radio, or Television, 18 U.S.C. § 1343 (1992).

property.[159] This statute has been held to include fraudulent use of telephone services.[160] Presumably, this statute may also cover 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 section 1346 of the Mail Fraud Chapter,[161] which specifically covers schemes to defraud.[162] Some state laws exist to punish theft of local telephone service or publication of telephone access codes.[163]

H. Viruses

As pointed out in the introduction, computer viruses are increasingly of concern — both for operators of computer information systems, as well as for users of the 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.[164] Computer virus crime involves an intent to cause damage, "akin to vandalism on a small scale, or terrorism on a grand scale."[165] Viruses can spread through networked computers or by sharing disks between computers.[166] Viruses cause damage by either attacking another file or by simply filling up the computer's memory or by using up the computer's processor power.[167] 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).[168] 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 the distinctions between worms and viruses.[169] Regardless, a worm is a program

---

[159] *Id.*

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

[161] 18 U.S.C. § 1346.

[162] *Id.*

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

[164] *See, e.g.*, Daniel J. Kluth, *The Computer Virus Threat: A Survey of Current Criminal Statutes*, 13 HAMLINE L. REV. 297 (1990).

[165] *Id.*

[166] David R. Johnson et al., *Computer Viruses: Legal and Policy Issues Facing Colleges and Universities*. 54 EDUC. L. REP. (West) 761 (Sept. 14, 1989).

[167] *Id.* at 762.

[168] *Id.*

[169] Eric Allman, *Worming My Way; November 1988 Internet Worm*, UNIX REV., January 1989, at 74.

specifically designed to move through networks.[170] 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, worms are defined as, "computer virus programs ... [which] propagate on a computer network without the aid of an unwitting human accomplice. These programs move of their own volition based upon stored knowledge of the network structure."[171]

Another type of virus is the "Trojan Horse."[172] These are viruses which hide inside another seemingly harmless program.[173] Once the Trojan Horse program is used on the computer system, the virus spreads.[174] The virus type which has gained the most fame recently has been the Time Bomb, which is a delayed action virus of some type.[175] This type of virus has gained notoriety as a result of the Michelangelo virus. A virus designed to erase the hard drives of people using IBM compatible computers on the artist's birthday, Michelangelo was so prevalent, it was even distributed accidentally by some software publishers when the software developers' computers became infected.[176]

One concern many have about statutes dealing with computer viruses is the problem that the statutes need some kind of intent requirement.[177] Without some sort of intent requirement, virus statutes may be sufficiently overbroad so as to cover defective computer programs.[178]

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.[179] If a virus also involves unauthorized access to an electronic communications system involving interstate commerce, the Electronic Communications Privacy Act may come into play.[180] Most states have statutes that make it a crime to

---

[170] Kluth, *supra* note 164, at 298.

[171] *Id.* at note 14.

[172] *See* Stover, *supra* note 32.

[173] *Id.*

[174] Kluth, *supra* note 164, at 298.

[175] *See* Stover, *supra* note 32.

[176] *Electronic Mail Software Provider Reports Virus Contamination*, UPI, Feb. 3, 1992, *available in* LEXIS, Nexis Library, UPI File.

[177] *See* Kluth, *supra* note 164.

[178] *Id.*

[179] 18 U.S.C. § 1030 (1984).

[180] Electronic Communications Privacy Act of 1986, 18 U.S.C. §2510 (1984).

intentionally interfere with a computer system.[181] These statutes will often cover viruses as well as other forms of computer crime. State statutes generally work by affecting any of ten different areas:[182]

1. Expanded definitions of "property" to include computer data.[183]
2. Prohibiting unlawful destruction of computer files.[184]
3. Prohibiting use of a computer to commit, aid or abet commission of a crime.[185]
4. Creating crimes against intellectual property.[186]
5. Prohibiting knowing or unauthorized use of a computer or computer services.[187]
6. Prohibiting unauthorized copying of computer data.[188]
7. Prohibiting the prevention of authorized use.[189]
8. Prohibiting unlawful insertion of material into a computer or network.[190]
9. Creating crimes like "Voyeurism"— Unauthorized entry into a computer system just to see what is there.[191]
10. "Taking possession" of or exerting control of a computer or software.[192]

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.[193] "[A SYSOP] might still be found liable on the

---

[181] Johnson et al., *supra* note 166, at 764. *See* Anne W. Branscomb, *Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime*, 16 RUTGERS COMPUTER TECH. L.J. 1, 30-31, 61 (1990).

[182] Branscomb, *supra* note 181, at 32.

[183] *Id.*

[184] *Id.* at 33.

[185] *Id.*

[186] *Id.* at 34.

[187] *Id.*

[188] *Id.* at 35.

[189] *Id.*

[190] *Id.*

[191] *Id.* at 36.

[192] *Id.* at 37.

[193] *See* Johnson et al., *supra*, note 166, at 764, 766.

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."[194] The nature of "care" still has not been defined by court or statute.[195] 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.

I. *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 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.[196] There must then be a breach of that duty[197] — the SYSOP must display conduct "which falls below the standard established by law for the protection of others against unreasonable risk of harm."[198] 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 foreseen and planned for — will not result in liability.[199] 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."[200] 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 what data and which services.

---

[194] *Id.* at 766.

[195] *Id.*

[196] W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS \30(1), at 164 (5th ed. 1984).

[197] *Id.* § 30(2), at 164.

[198] *Id.* § 31, at 169.

[199] *Id.* § 29, at 162.

[200] Cheryl S. Massingale & A. Faye Borthick, *Risk Allocation for Computer System Security Breaches: Potential Liability for Providers of Computer Services*, 12 W. NEW ENG. L. REV. 167, 187 (1990).

SYSOPs also have a duty to explain to each user the extent of his or her authorization to use the computer information service.[201]

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.

IV. 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 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 users' communications really are, and who may have access to the users' "personal" E-mail. The same is true for stored computer files. Just as importantly, System Operators should be aware of what restrictions and requirements exist to maintain users' privacy expectations.

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

One of the most significant cases establishing privacy for electronic communications is *Katz v. United States*.[202] *Katz* involved the use of an electronic listening device (or "bug") mounted on the outside of a public telephone booth.[203] The government (who placed the bug) assumed 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.[204] However, Defendant argued that the bug was an unlawful search and seizure in violation of the Fourth Amendment.[205] 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 constitu-

---

[201] *Id.* at 188-89.

[202] Katz v. United States, 389 U.S. 347 (1967).

[203] *Id.* at 348.

[204] *Id.* at 351.

[205] *Id.*

tionally protected."[206] 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.[207] 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.[208] For example, most people have a reasonable expectation that calls made from inside a closed telephone booth will be private. For computer users, this means 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.[209]

Statutory protection of the right to privacy was originally provided by the Federal Wiretap Statute.[210] However, this statute affected only "wire communication," which is limited to "aural [voice] acquisition."[211] In *United States v. Seidlitz*,[212] the court held that interception of computer transmission is not an "aural acquisition" and, therefore, the Wiretap Act did not provide protection.[213] Even if the Act did cover transmission, it still does not cover stored computer data.[214] This does not result in significant or comprehensive protection of E-mail or stored data.

B. *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 Amend-

---

[206] *Id.*

[207] *See, e.g.*, Oliver v. U.S. 466 U.S. 170 (1984).

[208] *See* 389 U.S. at 347; *see also* California v. Ciraolo 476 U.S. 207, *reh g denied*, 478 U.S. 1014 (1986).

[209] *See* Ruel Hernandez, *Computer Electronic Mail and Privacy, available over Internet, by anonymous* FTP, at FTP.EFF.ORG (Electronic Frontier Foundation).

[210] 18 U.S.C. § 2510 (1968).

[211] *See* Hernandez, *supra* note 209.

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

[213] *Id.* at 157.

[214] *See* Hernandez, *supra* note 209.

> ment's protection on its head. The Supreme Court had 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.[215]

The Federal Wiretap Act was updated by the Electronic Communications Privacy Act of 1986.[216] The Electronic Communications Privacy Act deals specifically with the interception and disclosure of interstate[217] electronic communications[218] , and 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 prosecuting anyone who will not respect that privacy. The statute provides in part that "any person who (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication"[219] shall be fined or imprisoned.[220] 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.[221] 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[222] provides an exception for SYSOPs and their employees to the extent necessary to manage properly the computer information system:

> 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

---

[215] Robert W. Kastenmeier et al., *supra* note 8, at 720 (citations omitted).
[216] Electronic Communications Privacy Act of 1986, 18 U.S.C. §2510 (1968).
[217] *Id.* § 2510(12).
[218] 18 U.S.C. § 2511.
[219] *Id.* § 2511(1)(a).
[220] *Id.* § 2511(4).
[221] *Id.* § 2511(1)(c).
[222] *Id.* § 2511(2)(a)(i).

> 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 wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.[223]

"Electronic Communication System" is defined as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."[224] Further exceptions are made for SYSOPs of these systems when the originator or addressee of the message gives consent;[225] when the message is being given to another service provider to be further forwarded towards its destination;[226] where the message is inadvertently obtained by the SYSOP; and appears to pertain to a crime;[227] when the divulgence is being made to a law enforcement agency;[228] or where the message is configured so as to be readily accessible to the public.[229] 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).[230] 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.[231]

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.[232] The statute does not prohibit the use of pen registers or trap and trace devices.[233] The

---

[223] *Id.*

[224] *Id.* § 2510(14).

[225] *Id.* § 2511(3)(b)(ii).

[226] *Id.* § 2511(3)(b)(iii).

[227] *Id.* § 2511(3)(b)(iv).

[228] *Id.* § 2511(3)(b)(iv).

[229] *Id.* § 2511(3)(b)(i).

[230] *Id.* § 2511.

[231] 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.

[232] 18 U.S.C. § 2518 (1968).

[233] *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.

warrant requirement 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.

C. *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.[234] The section reads, in part, "whoever -- (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"[235] shall be subject to fines and/or imprisonment, or both.[236] Like section 2511, this section includes provisions prohibiting the divulgence of the stored messages.[237] Importantly, while this statute allows law enforcement agencies to gain access to stored communications, subject to a valid search warrant,[238] 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.[239] Such a statute is needed because the government often takes the stored data to sort through during the course of its investigation, as was the case in *Steve Jackson Games, Inc. v. United States Secret Service*.[240] In this case, the Secret Service raided a publisher and seized its bulletin board system, electronic mail and all. The court held that the government had to go through the procedures established by section 2701 *et seq.*, covering stored wire and electronic communications, in order to discover

---

[234] Id. § 2701.

[235] Id. § 2701(a).

[236] Id. § 2701(b).

[237] Id. § 2702.

[238] *See id.* § 2703.

[239] Id. § 2703(a)

[240] Steve Jackson Games, Inc. v. United States Secret Serv., 816 F. Supp. 432 (W.D. TEX. 1993).

properly the contents of the electronic mail on the BBS.[241] The court said that the evidence of good faith reliance on what the Secret Service believed to be a valid search warrant was insufficient.[242] The government *knew* that the computer had private electronic communications stored on it, and therefore the only means they could legally use to gain access to those communications was by compliance with the Act, and not by seizing the BBS.[243]

The Steve Jackson Games Case was also valuable for showing the interplay between protection against interception of electronic communication[244] and access to stored communication.[245] Judge Sparks held, in essence, that taking a whole computer is not an "interception" as contemplated by section 2510 *et seq.*, especially in light of the protection of stored communication by section 1701 *et seq.* He analogized the situation to the seizure of a tape recording of a telephone conversation and said that the "aural acquisition" occurs when the tape is made, not each time the tape is played back by the police.[246] This interpretation of an intellectually complex concept[247] makes sense when the two code sections are read together.

D. *An Apparent Exception for Federal Records*

A recent case presents an apparent exception to the Electronic Communications Privacy Act.[248] In *Armstrong v. Executive Office of the President,*[249] while not mentioning the Electronic Communications Privacy Act, the court required certain electronic mail and stored data to be saved and made available for the National Archives.[250] While electronic communications are normally

---

[241] *Id.* at 434.

[242] *Id.* at 443.

[243] *Id.* at 442-43.

[244] *Id.*; 18 U.S.C. § 2510.

[245] 816 F. Supp. at 442-43.

[246] 816 F. Supp. at 441-42; 18 U.S.C. § 2701.

[247] Stored communications may be intercepted in some sense because the message writer may have sent the E-mail, but it has not yet been read by the recipient. Also, messages being sent from one BBS user to another on bulletin board systems which support multiple users simultaneously may never be stored on the computer. By reading the two sections as complimentary, the complexities should be accounted for - communications not covered by § 2510 should be covered by § 2701 and vise versa.

[248] *See* 18 U.S.C. § 2511 (1968).

[249] Armstrong v. Executive Office of the President, 810 F. Supp 335 (D.C. Cir. 1993).

[250] *Id.* at 348.

protected under the Electronic Communications Privacy Act, the Federal Records Act[251] requires that:

> all ... machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States under Federal law or in connection with the transaction of public business and preserved or appropriated for preservation by that agency ... as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them [be preserved].[252]

The court held that the actual computer records must be saved, not just paper copies of the electronically mailed notes, because the computer records contain more information than printouts.[253] Printed copies of the messages contain the text of the notes, but only the computer records contain information such as who received the E-mail messages and when the communication was received.[254]

A similar possible exception to the privacy of E-mail is the Presidential Records Act,[255] which requires that all records classified by the Act as "Presidential Records"[256] be preserved for historical researchers. However, the only case to apply this statute to Presidential E-mail held that the Presidential Records Act impliedly precludes judicial review of the President's compliance with the Act.[257]

E. *Privacy Protection Act of 1980*

It is also possible that computer information systems will be

---

[251] Federal Records Act, 44 U.S.C. §§ 2101-2118, 2901-2910, 3101-3107, 3301-3324.

[252] *Id.* § 3301.

[253] 810 F. Supp. at 342, 343.

[254] *Id.* at 341.

[255] 44 U.S.C. § 2201.

[256] Section 2201(2) of the Act defines a Presidential record as:

> documentary materials ... created or received by the President, his immediate staff, or a unit or individual in the Executive Office of the President whose function is to advise and assist the President, in the course of conducting activities which relate to or have an affect upon the carrying out of the constitutional, statutory, or other official or ceremonial duties of the President.

Id.

[257] Armstrong v. Bush, 924 F.2d. 282, 290 (D.C. Cir. 1991).

protected under the Privacy Protection Act of 1980.[258] 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."[259] This statute was passed to overturn the decision in *Zurcher v. Stanford Daily*,[260] a case which held that a newspaper office could be searched, even when no one working at the paper was suspected of a crime.[261] The only exceptions to the law's prohibition on searches of publishers are the following: probable cause to believe that the person possessing the materials has committed or is committing the crime to which the materials relate,[262] or the immediate seizure is necessary to prevent the death or serious injury to a human being.[263] Based on the list of types of "publishers" covered by this statute, electronic publishers should fall under this section.

The first case that attempted to apply this statute to electronic publishers was the *Steve Jackson Games* case, mentioned in the preceding section. It is a good case study in law enforcement violations of electronic data privacy. Steve Jackson Games is a small publisher of fantasy role-playing games in Texas.[264] The company also ran a BBS to gain customer feedback on the company's games.[265] 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 etc.).[266] 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."[267] The raid by the Secret Service caused the company to temporarily shut down;[268] Steve Jackson Games also had to lay off half its employees.[269] The release of

---

[258] Privacy Protection Act of 1980, 42 U.S.C. § 2000aa (1980).

[259] *Id.* § 2000aa(a).

[260] Zurcher v. Stanford Daily, 436 U.S. 547 (1978).

[261] *Id.* at 549.

[262] 42 U.S.C. §2000aa(a)(1).

[263] *Id.* §2000aa (a)(2).

[264] Mitchell Kaypor, *Civil Liberties in Cyberspace; Computers, Networks and Public Policy*, SCI. AM., Sept. 1991, 158, 158.

[265] *Id.*

[266] Steve Jackson Games, Inc. v. United States Secret Serv., 816 F. Supp. 432, 439 (W.D. Tex. 1993).

[267] *Id.* at 439-40.

[268] *Id.* at 438.

[269] *Id.*

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.[270] The Electronic Frontier Foundation, which provided legal counsel for Steve Jackson, likened the Secret Service's action to an indiscriminant seizure of all of a business's filing cabinets and printing presses.[271] 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.[272] The document contained information which was publicly available in other forms.[273] 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.[274] The employee was also co-SYSOP of the bulletin board system at Steve Jackson Games.[275] The case held that at the time of the raid, the Secret Service did not know that Steve Jackson Games was a publisher (even though they should have), as the Privacy Protection Act[276] requires, though they did know shortly after.[277] Judge Sparks said the continued refusal to return the publisher's work product, once the Secret Service had been informed that Steve Jackson Games was a publisher, amounted to a violation of the Act.[278] In the raid, the Secret Service seized a number of Steve Jackson's computers, and a number of papers.[279] As mentioned, this included the company's BBS, which contained public comments on newspaper articles submitted for review, public announcements, and other public and private communications.[280]

While the judge did find a violation of the Privacy Protection Act,[281] he did not specify which items led to the violation. The vio-

---

[270] *Legal Case Summary*, May 10, 1990, *available over Internet*, by anonymous FTP, at FTP.EFF.ORG (Electronic Frontier Foundation).

[271] *Id.*

[272] 816 F. Supp. at 436.

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

[274] *Special Issue: Search Affidavit for Steve Jackson Games*, COMPUTER UNDERGROUND DIG., Nov. 13, 1990, *available over Internet*, by anonymous FTP, at FTP.EFF.ORG (Electronic Frontier Foundation).

[275] 816 F. Supp. at 436.

[276] 42 U.S.C. § 2000aa.

[277] 816 F. Supp. at 437.

[278] *Id.*

[279] *Id.*

[280] *Id.* at 439-40.

[281] *Id.* at 441.

lation could have been the seizure of the papers, the computers used for word processing, or the BBS. Thus, the question still remains unanswered as to whether the seizure of the BBS alone, which was being used to generate work product for the publisher, would have amounted to a violation of the Act. Importantly, other users of the BBS who had posted public comments about Steve Jackson's Games were also plaintiffs in the case. They were not allowed recovery based on the Privacy Protection Act.[282] Therefore, either the individual message posters were not considered to be publishers themselves (only perhaps authors of works published in electronic form by Steve Jackson Games' BBS) or their messages were not considered to be work product subject to protection.

V. 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.[283]

A. *Obscenity*

The constitutional definition of "obscenity," as a term of art,[284] was solidified in *Roth v. United States*.[285] The *Roth* definition asks if the material deals with sex in a manner appealing to prurient interests.[286] This standard was further explained in *Miller v. California*,[287] a case which explored the constitutionality of a state statute prohibiting the mailing of unsolicited sexually explicit material.[288] The court expressed the test for obscenity as:

> whether (a) the average person, applying community standards

---

[282] *Id.*

[283] *See, e.g.*, F.C.C. v. Pacifica Foundation, 438 U.S. 726, *reh'g denied*, 439 U.S. 883 (1978).

[284] The term "obscene material" is used synonymously with "pornographic material." *See* Miller v. California, 413 U.S. 15, n.2, *reh'g denied*, 414 U.S. 881 (1973).

[285] Roth v. United States, 354 U.S. 476 (1957).

[286] *Id.* at 487.

[287] 413 U.S. at 15.

[288] *Id.*

> 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.[289]

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.[290] 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.[291] 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 states are free to make laws severely restricting its availability, especially to children.[292] Although states can regulate the availability of obscene material, they cannot forbid the mere possession of it in the home.[293] The justification for this is based on privacy.[294] In the now famous words of Justice Marshall in *Stanley v. Georgia*,[295]

> 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 what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds.[296]

Stanley has been interpreted as establishing a "zone of privacy" about one's home.[297] 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.[298] However,

---

[289] *Id.* at 24.

[290] Pope v. Illinois, 481 U.S. 497, 500 (1987) (citing Smith v. United States, 431 U.S. 291 (1977)).

[291] Hamling v. United States, 418 U.S. 87 (1974).

[292] *See, e.g.*, 413 U.S. 15; Kois v. Wisconsin, 408 U.S. 2219 (1972).

[293] Stanley v. Georgia, 394 U.S. 557 (1969).

[294] *Id.* at 565.

[295] *Id.*

[296] *Id.*

[297] Jensen, *supra* note 7.

[298] Note that an exception would be made for child pornography, *see* discussion *supra* part III.D.

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.[299] Support for this argument comes from U.S. *v. Orito*[300] which held that Congress has the authority to prevent obscene material from entering the stream of commerce, either by public or private carrier.[301] 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 bookstore.[302] *Stanley*[303] 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."[304]

B. *Indecent Speech*

Speech which is not considered obscene may qualify as indecent. In F.C.C. *v. Pacifica Foundation, Inc.*, the court held that 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.[305] Indecent language is that which "describes, in terms patently offensive as measured by community standards ... sexual or excretory activities and organs ..."[306] This language comes from F.C.C. *v. Pacifica Foundation, Inc.*,[307] 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.

---

[299] Jensen, *supra* note 7.

[300] U.S. v. Orito, 413 U.S. 139 (1973).

[301] *Id.* at 143.

[302] *See* Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).

[303] 394 U.S. at 565.

[304] Paris Adult Theatre I v. Slaton, 413 U.S. 49, 68-69, *reh g denied*, 414 U.S. 881 (1973).

[305] 438 U.S. at 726.

[306] *Id.* at 732.

[307] *Id.* at 726-27.

VI. COPYRIGHT ISSUES

A. Basics of Copyrights

Text, pictures, sounds, software — all of these can be distributed by computer information systems, and all can be copyrighted. The Constitution guarantees 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."[308] This power is exercised in the form of the Copyright Act, Title 17 of the U.S. Code.[309] 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."[310] The statute lists several types of works as illustrations of types of works which qualify for copyright protection.[311] Relevant to computer information systems, the list includes literary works; pictorial, graphic, and sculptural works; motion pictures and other audiovisual works; and sound recordings.[312] 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.[313] 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."[314] 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.[315] This can lead to some strange results. A live concert cannot be copyrighted under this statute, but if the performer records the concert while he or she performs, the concert can then be copyrighted.[316] For computer information systems,

---

[308] U.S. CONST. art. I, § 8, cl. 8.

[309] Copyright Act of 1947, 17 U.S.C. § 101 (1947).

[310] *Id.* § 102(a).

[311] *Id.* § 101.

[312] *Id.* § 102(a) Other categories include musical works, dramatic works, pantomimes and choreographic works, and architectural works. *Id.*

[313] *See* § 101 (Historical and Statutory Notes).

[314] *Id.*

[315] *Id.*

[316] *Id.*

this implies that conversations occurring over a computer or network which are not stored on a disk[317] are unprotected by the Copyright Act, but if any 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.[318] 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.[319] Postscript fonts, on the other hand, consist of a computer program which describes the outline of the letter.[320] 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.[321] Postscript fonts are seen as computer programs—the program is a work of authorship, it just so happens to draw letters, and they have been held to be copyrightable.[322]

The Copyright Act gives the copyright holder exclusive rights to his or her works.[323] 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.[324] 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 personally, but two problems exist regarding material that users

---

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

[318] Id. § 102(b).

[319] See Charles Von Simon, *Page Turns in Copyright Law with Adobe Typeface Ruling*, COMPUTERWORLD, Feb. 5, 1990, at 120.

[320] Id.

[321] See *Adobe Successfully Registers Copyright Claim for Font Program*, COMPUTER LAWYER, Feb. 1990, at 26.

[322] Von Simon, *supra* note 319.

[323] Copyright Act of 1947, 17 U.S.C. § 106 (1947).

[324] Id.

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 participant in the copyright infringement by allowing the computer file to be distributed on his or her system.[325] 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.[326] Even subconscious copying has been held to be an infringement.[327]

One protection the Copyright Act gives to a computer information system is a compilation copyright. A compilationn copyright gives the SYSOP a copyright on the data contained in the computer information system as a whole.[328] 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.[329] 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, for example, to the arrangement of the articles which makes up the periodical as a whole.[330] A bulletin board system could presumably also copyright its entire message base.

As mentioned, the Copyright Act gives an author the exclusive rights to make copies of his or her works, as well as create derivative works.[331] This includes copies in computer readable form.[332] Thus, scanned pictures, digitized sounds, machine readable texts,

---

[325] *See* Screen Gems-Columbia Music, Inc. v. Mark-Fi Records, Inc., 256 F. Supp. 399 (S.D.N.Y. 1966).

[326] De Acosta v. Brown, 146 F.2d 408 (2d Cir. 1944).

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

[328] 17 U.S.C. § 103.

[329] *Id.*

[330] Feist Publications, Inc. v. Rural Tel. Serv. Co., Inc., 111 S.Ct. 1282 (1991).

[331] 17 U.S.C. § 106.

[332] 17 U.S.C. § 101.

and computer programs are all subject to an author's copyright. Any attempt to turn original material into one of these computer-readable forms without the author's permission (and unless the copy falls under one of the exceptions in sections 107-120) is a violation of the author's copyright.

With decreasing costs of data storage, and increasing access to computer networks, comes an increase in the number of computer archives. These computer archives store various types of data which can be searched by the archive user. The archive site can be searched, and the information can be copied by anyone with sufficient access to the archive. This ease with which information can be accessed and duplicated has some profound copyright implications. I will use as an example a "lyric server," an archive that stores lyrics to songs by assorted artists. Other types of information that can be distributed will be discussed shortly.

In my lyric server example, if someone is sitting down with an album jacket and typing the lyrics into the computer for distribution in the archive, the translation of the lyrics from the album jacket to a computer text file constitutes an unauthorized copy. Similarly, if someone else types in the file and a System Operator then puts the file into the archive for distribution, the SYSOP has violated the author's right to make and distribute copies of his or her work.[333]

Once the file is in the archive for distribution, every time the information is copied, there may be a copyright violation. There is a difference here between copying and viewing. As mentioned, the Copyright Act protects against unauthorized copying of a work. The Act defines a copy as a fixation "from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device."[334] Thus, if someone connects to the computer information system and just peruses the archive, if the information is not "downloaded," "screen captured," or otherwise recorded on computer disk, tape, or printout, then no fixation is made and thus, no copy. However, while the archive user may not be making a copy, if the archive is publicly accessible viewing some types of files may constitute a public performance or display[335] of the copyrighted work, which are also protected rights.[336]

---

[333] 17 U.S.C. §§ 106(1), (3).

[334] 17 U.S.C. § 101

[335] *Id.*

[336] 17 U.S.C. § 106

Whether the unauthorized archiving of a copyrighted work or whether further copying of a protected work by the archive user constitutes a violation of section 106 of the Copyright Act is also determined by whether the copying falls under one of the Act's exceptions. The two relevant exceptions are the "fair use" provision[337] and the "reproduction by libraries and archives" provision.[338]

> [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 is decided in each case as a matter of equity ... ."[339]

The fair use provision contains a list of uses that are presumed to be acceptable uses of copyrighted works, and a list of four factors that must be taken into account to determine if the use constitutes a fair use of the work. The list includes use for criticism, comment, news reporting, teaching, scholarship, or research.[340] This list may provide some guidance as to what constitutes legal use for the *user* of a computer information system, but not for the *provider* of the archive. The archive user may be safe in copying song lyrics from the lyric server if he or she is using the lyrics for the purpose of commentary, for example, but the SYSOP who provides the service may not have the same defense.

The four factors to be applied in deciding whether the use of a copyrighted work in each case constitutes fair use are:

> (1) the purpose and character of the use, including whether such use is of commercial nature or is for nonprofit purposes:
> (2) the nature of the copyrighted work;
> (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
> (4) the effect of the use upon the potential market for or the value of the copyrighted work.[341]

Applying these factors to the System Operator's liability for a lyric server, the character of the use depends on whether access to the

---

[337] 17 U.S.C. § 107.

[338] 17 U.S.C. § 108.

[339] Bruce J. McGiverin, Note, *Digital Sound Sampling, Copyright and Publicity: Protecting Against the Electronic Appropriation of Sounds*, 87 COLUM. L. REV. 1723, 1736 (1987) (citations omitted).

[340] 17 U.S.C. § 107.

[341] *Id.*

lyrics is available for free, or as a profit making venture. The nature of the work is song lyrics, likely intended for commercial sale. The amount used, is the entire lyrics to each copyrighted song.[342] 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. And finally, placing copyrighted lyrics on a publicly accessible computer information system may have a profound impact on the potential market for the computerized distribution of lyrics, depending upon the potential number of users of the lyric server.

The other possible exception to the copyright holder's exclusive rights is section 108 which deals with copying by libraries and archives.[343] Unlike the section 107 fair use provision, which in this case is more aimed at the end user, section 108 is aimed more at the information provider. Section 108 allows the archive itself to reproduce or distribute no more than one copy or phonorecord of a work, and as long as the archive is available to the public or to researchers not affiliated with the library or archive, the archive does not get direct or indirect profit from making or distributing the copy, and the copy contains a notice of copyright.[344] It is reasonable to argue that when the user requests a host computer to send a text file containing the lyrics to a specific song, the archive is making this type of copy. Section 108 allows the user to request copies of "no more than one article or other contribution to a copyrighted collection or periodical issue, or ... a small part of any other copyrighted work"[345] as long as the copy becomes the property of the user, the archive has no notice that the copy is to be used for anything other than study, scholarship, or research, and as long as the archive displays prominently "at the place where orders are accepted, and includes on its order form, a warning of copyright in accordance with requirements that the Register of Copyrights shall prescribe by regulation."[346] This requirement of the posting of copyright notice would clearly apply to the lyric server, just as it does to a library photocopier. Even if a passive computer system is held to be more like a self-serve copier, and the SYSOP

---

[342] While the use of the entire song's lyrics weighs heavily against the use being a fair use" the Supreme Court has held that use of the entire work can be a fair use. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984).

[343] 17 U.S.C. § 108.

[344] 17 U.S.C. § 108(a).

[345] 17 U.S.C. § 108(d).

[346] *Id.*

plays no part in the copying by the user, if the archive is made available so that copying may occur, the system operator is still subject to a copyright infringement claim if the "reproducing equipment" does not bear a notice that any copies made may be subject to copyright law.[347]

To summarize with the lyric server example, while a system operator may not be liable for the use to which users put any copyrighted text they copy off of the computer information system, the SYSOP still must be wary of some obstacles. Copyright notice must be provided, and, specifically, the notice that is prescribed by the Register of Copyrights may require that each file have its own copyright notice. Access to the archive must be fairly open. The archive must not directly or indirectly profit from distributing the copyrighted works. Potentially the biggest hurdle is that care must be taken in assembling the archive so that any materials that need to be converted into a computer-readable form are converted without violating the author's section 106 rights.[348]

B. *Copyrighted Text*

Copyrighted text can appear on computer information systems as either files in a file server or database; or it can appear in an E-mail message or post on a BBS; or it can be worked into 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 as a conspirator in the copyright infringement.[349]

C. *Copyrighted Software*

Bulletin board systems, network file servers, and main-frame 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

---

[347] 17 U.S.C. § 108(f)(1).

[348] *See* 17 U.S.C. § 106.

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

lawsuit if any of that copied software is copyrighted.[350] The SPA is a group established by a number of software publishers in order to cut down on software piracy.[351] The SPA monitors bulletin board systems for distribution of copyrighted software.[352] 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.[353] The SPA also examines office computers for unlicensed software.[354]

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.[355] Compliance with the SPA requirements saves the offender the additional cost of a lawsuit.[356] Noncompliance will result in a lawsuit filed by the SPA.[357]

As mentioned, not all copying of copyrighted software is illegal. Two exceptions are worth noting. One is for the making of 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.[358] The Act also allows a copy to be 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."[359] 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.[360] 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 specified in the documentation distributed with the

---

[350] Janet Mason, *Crackdown on Software Pirates; Industry Watchdogs Renew Efforts to Curb Illegal Copying*, COMPUTERWORLD, Feb. 5, 1990, at 107.

[351] *Id.*

[352] *Id.*

[353] *Id.*

[354] *Id.*

[355] *Id.*

[356] *Id.*

[357] *Id.*

[358] 17 U.S.C. § 117(1).

[359] *Id.* § 117(2).

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

software) without payment of the shareware fee is a violation of copyright law.[361]

D. *Copyrighted Pictures*

As mentioned earlier,[362] 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, they can be further altered with image processing software.[363] All of these forms are covered by the Copyright Act.[364] Pictures created on the computer using graphics or "paint box" software are in an original copyrightable form.[365] Images that are scanned are in violation of the original copyright holder's rights, unless permission to distribute the scanned image has been obtained.[366] In fact, even the unauthorized initial scan made of a copyrighted work is in violation of the copyright, even without further distribution.[367] 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."[368] Images which are scanned that are not copyrighted, such as works on which the copyright has already expired,[369] do not violate the Copyright Act, and, if sufficient creativity is contributed in the scanning process, the images may be eligible for copyright protection in their own right.[370] If a scan of a copyrighted picture is then altered into a new image, the modified version likely still falls

---

[361] *Id.*

[362] *See supra* text accompanying notes 114-16.

[363] Legal aspects of the doctoring of photographs are beyond the scope of this paper — for a good discussion of such issues, see Benjamin Seecof, *Scanning into the Future of Copyrightable Images: Computer-Based Image Processing Poses a Present Threat*, 5 HIGH TECH. L.J. 371 (1990).

[364] 17 U.S.C. § 102(a)(5).

[365] *Id.* § 102(a).

[366] *Id.* § 101 (defining a copy); *id.* § 106 (Section 106 gives the copyright holder exclusive rights to make copies and derivative works of his or her creation.).

[367] *Id.* § 101.

[368] Ezra Shapiro, *More on Copyright; Digitizing of Copyrighted Images*, MACWEEK, Oct. 11, 1988, at 27.

[369] 17 U.S.C. § 302 (applying to works created after Jan. 1, 1978, provides that a copyright shall expire 50 years after the death of the author of the work).

[370] *See, e.g.*, Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53 (1984) (holding that photographs are copyrightable by virtue of the creativity that goes into arranging the subject elements and photographic variables into a distinct picture).

under the original copyright.[371] It therefore enjoys no protection on its own, and copyright release must be obtained from the holder of the copyright in order to distribute the image (or to modify it in the first place).[372]

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).[373] Based on these rights, a SYSOP should be especially careful of images which appear to be doctored. Many of the larger computer information services settle the dilemma over establishing copyright status by allowing the images under the assumption that no one will mistake a scanned copy for an original, and that therefore no one is being hurt.[374] This argument has no basis in the law of copyrights. The Copyright Act gives the author the right to make copies of his or her work, and this includes bad copies.[375] 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.[376]

Computerized images present a whole new market for an artist's work, and widespread, unauthorized distribution can destroy the potential to disseminate the work in the computer market — a right clearly given to the author of the work. Some computer information services also defend the possibility that some of their stored images are provided on the basis of the "fair use"[377]

---

[371] 17 U.S.C. § 106; *see* Gracen v. Bradford Exch., 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).

[372] *Id.* § 106A.

[373] *Id.*

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

[375] 17 U.S.C. § 106.

[376] Franklin Mint Corp. v. National Wildlife Art Exch., 575 F.2d 62 (3d Cir. 1978); *see also* Zaccini v. Scripps-Howard Broadcasting Co., 433 U.S. 562 (1977) (involved TV station covering 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).

[377] 17 U.S.C. § 107.

exception.[378] Relying on fair use is also not a very realistic position to take. One artist found some of his work scanned and available on a BBS, only 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.[379] Such wide infringement into a potentially new market for the artist 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 above analysis applies to sampled sounds, as well as images, 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 the tort of unfair competition.[380] 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.[381]

VII. LIABILITY FOR COMPUTER INFORMATION SYSTEM CONTENT

In order to determine who is liable for illegal activity of the kind so far discussed, 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 unique media. Specific legislation geared towards the computer media has already been discussed. However, the law still leaves some issues unresolved. To resolve such issues, it is necessary to understand how other media are regulated, and how computer information systems are similar to or different from those media.

---

[378] Shapiro, *supra* note 374.

[379] Liz Horton, *Electronic Ethics of Photography: Use of Images in Desktop Publishing*, FOLIO: THE MAG. FOR MAG. MGMT., Jan. 1990, at 71.

[380] Thomas C. Moglovkin, Note, *Original Digital: No More Free Samples*, 64 S. CAL. L. REV. 135, 163 (1990).

[381] *Id.* at 165.

In all cases where the law would hold a party guilty for actions carried out on a computer information system, this paper 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 SYSOP's 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 do when they are published.

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.[382] 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.[383] 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,[384] the protection is not complete. All of the restrictions on content discussed earlier apply to publishers —advocacy of lawless

---

[382] Mitchell Kapor, *A Day in the Life of Prodigy*, EFFECTOR ONLINE, *available over* Internet, by anonymous FTP, at FTP.EFF.ORG (Electronic Frontier Foundation) (Vol. 1, No. 5).

[383] Robert Charles, *Computer Bulletin Boards and Defamation: Who Should be Liable? Under What Standard?*, 2 J.L. & TECH 121, 131 (1987).

[384] U.S. CONST. amend. I.

action, child pornography, obscenity, defamation, etc. The SYSOP, as an electronic publisher, shares the same liability as a print publisher would, for example, the *New York Times*[385] "actual malice" standard for defamation, and a "knowing" standard as required by the statutes forbidding the transportation of material involved in child pornography.[386] 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 generally requires the publisher to have published the defamation with "knowing or reckless disregard for the truth."[387] 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 "knowing or reason to know" standard. An argument for this minimum requirement is supported by some cases, for example, those which do not allow the publisher to be held liable for everything in his or her periodical, such as the safety of products sold by their advertisers.[388] As the court in *Yuhas v. Mudge* 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."[389]

---

[385] New York Times v. United States, 403 U.S. 713 (1971).

[386] 18 U.S.C. § 2252.

[387] 403 U.S. at 713.

[388] *See, e.g.*, Yuhas v. Mudge, 322 A.2d 824, 825 (N.J. Super. Ct. App. Div. 1974).

[389] *Id.*

Operators of large systems are quick to support the view that the job of monitoring every communication on their systems would be a prohibitively large task.[390] 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 bulletin 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 contracting 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.[391] Unless the secondary publishers know or have reason to know of the defamatory nature of the material they are transmitting, they are free from liability for defamation.[392] Secondary publishers are often treated synonymously with republishers which are discussed in the next section.

---

[390] Information Policy, Computer Communications Networks Face Identity Crisis over Their Legal Status, DAILY REP. FOR EXECUTIVES, Feb. 26, 1991, at A-6.

[391] Joseph P. Thornton, et al., Symposium: Legal Issues in Electronic Publishing: 5. Libel, 36 FED. COM. L.J. 178, 179 (1984).

[392] See RESTATEMENT (SECOND) OF TORTS § 581 (1989).

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."[393] Some computer information systems are like republishers because all they do is make available files, just like a book seller 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, E-mail 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."[394]

The case that first established the immunity from liability for distributors, breaking the common law tradition, was *Smith v. California*.[395] *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, the court held that a law which holds a bookseller strictly liable for the contents of the books he or she sells is unconstitutional. Justice Brennan stated his reasons as follows:

> For if the bookseller is criminally liable without knowledge of the contents ... 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." 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

---

[393] Jensen, *supra* note 7, at 3.

[394] Charles, *supra* note 383, at 131.

[395] Smith v. California, 361 U.S. 147 (1959), *reh'g denied*, 361 U.S. 950 (1960).

> liability, thus would tend to restrict the public's access to forms of the printed word which the State could not constitutionally suppress directly.[396]

While this case did not determine the degree of liability appropriate for a bookseller, it did find that strict liability was too restrictive.[397] 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.[398] In addition, secondary publishers are not required to investigate the contents of the messages they are delivering in order to avoid liability.[399]

Recently, a court has applied the *Smith*[400] analysis to computer information systems. *Cubby, Inc. v. CompuServe, Inc.*[401] 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, founded in 1969 as a time-sharing system by H&R Block in order to make use of some of its surplus computer facilities.[402] 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.[403] The groups maintaining the forums are similar to print publishers — they take articles submitted by users and then 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 defamed the plaintiff.[404] CompuServe had no opportunity to review the periodical's contents before it was made available to CompuServe's subscribers.[405] 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

---

[396] *Id.* at 153 (citation omitted).

[397] *Id.* at 155.

[398] Seton v. American News Co., 133 F. Supp. 591 (N.D. Fla. 1955); *cf.* Manual Enters., Inc. v. Day, 370 U.S. 478 (1962).

[399] 133 F. Supp. at 593.

[400] 361 U.S. at 950.

[401] 776 F. Supp. at 135.

[402] Clifford Carlsen, *Wide Area Bulletin Boards Emerge as Method of Corporate Communications*, SAN FRANCISCO BUS. TIMES, Mar. 15, 1991, at 15.

[403] 776 F. Supp. at 137.

[404] *Id.* at 138.

[405] *Id.*

contained in the periodical, CompuServe was in essence "an electronic, for-profit library."[406] 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.[407]

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 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.[408]

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

---

[406] *Id.* at 140.

[407] *Id.*

[408] *The Compuserve Case: A Step Forward in First Amendment Protection for Online Services*, EFFECTOR ONLINE, Jan. 7, 1992, *available over Internet, by anonymous FTP, at* FTP.EFF.ORG (Electronic Frontier Foundation) (Vol. 2, No. 3).

> "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.[409]

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.[410]

Common carriers have generally been considered secondary publishers,[411] and as such, have traditionally functioned under a reduced standard of liability.[412] That standard is, once again, a "know or have reason to know" standard of liability.[413] This standard has been widely adopted and applied to the electronic communications media: from telegraph,[414] to telephone,[415] and even to options such as telephone answering services.[416] 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.[417] 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.[418] And a third reason is privacy; by removing a need for common carriers to monitor content of transmissions, the likelihood is increased that transmissions will be held private. 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

---

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

[410] *Id.* at 608.

[411] *E.g.*, Von Meysenbug v. Western Union Tel. Co., 54 F. Supp 100 (S.D. Fla. 1944); Mason v. Western Union Tel. Co., 52 Cal. App. 3d 429, (1975).

[412] RESTATEMENT (SECOND) OF TORTS § 612 (1989).

[413] *Id.* § 581.

[414] 54 F. Supp at 100; Western Union Tel. Co. v. Lesesne, 182 F.2d 135 (4th Cir. 1950); O'Brien v. Western Union Tel. Co., 113 F.2d 539 (1st Cir. 1940).

[415] Anderson v. New York Tel. Co., 320 N.E.2d 647 (N.Y. 1974).

[416] People v. Lauria, 251 Cal. App. 2d 471 (1967).

[417] Charles, *supra* note 383, at 143.

[418] *Id.* at 123.

common carrier.

Like a common carrier, computer networks carry data from one computer to another with no regard for the information being transferred. Data that is 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 is gained from the Electronic Communications Privacy Act of 1986[419] 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 guess 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 phone. 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.[420] An exception is made for indecent telephone messages, so long as provisions are used to prevent minors from receiving these indecent messages.[421] Allowable safeguards include: scrambling messages so they cannot be understood without a descrambler, issuing a password by mail with age verification, or requiring a credit card number before transmission of the message.[422] 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 connecting to a bulletin board system or other service 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.[423]

---

[419] Electronic Communications Privacy Act of 1986, 18 U.S.C. §2510.

[420] 47 U.S.C. § 223.

[421] 47 C.F.R. § 64.201

[422] *Id.*

[423] *See* Sable Communications v. F.C.C., 492 U.S. 115 (1989).

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 greater 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.[424] U.S. mail, or "snail mail" is governed by a statute which gives "regular" mail the same kind of privacy that the Electronic Communications Privacy Act[425] 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 the correspondence, or to pry into the business or secrets of another, or

---

[424] U.S. CONST. art. I, § 8.

[425] 18 U.S.C. § 2510.

> opens, secretes, embezzles, or destroys the same ... .[426]

This statute has the same effect as the statutes specifically geared towards electronic communications — it protects both mail in transmission,[427] as well as mail being stored for the recipient.[428] Just as the Electronic Communications Privacy Act protects stored communications in the form of an E-mail recipient's "mail box,"[429] so does the postal service protect a "snail mail" recipient's mail box.[430] 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.[431] However, the reason for this protection from unpleasant U.S. mail — based on notions of trespass[432] — 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 and reject any 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.[433] 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 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

---

[426] Mail, 18 U.S.C. § 1702.

[427] *Compare* § 1702 *with* E-mail, 18 U.S.C. § 2510.

[428] *Compare* § 1702 *with* § 2511.

[429] § 2511.

[430] § 1702; *see also* United States Postal Serv. v. Council of Greenburgh Civic Ass'n, 453 U.S. 114 (1981).

[431] Rowan v. United States Postal Dep't, 397 U.S. 728 (1970).

[432] *Id.* at 737.

[433] Bolger v. Young Drug Prods. Corp., 463 U.S. 60 (1983).

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 (1601) 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."[434] A fairly modern case (1937) which is cited more frequently in this country is *Byrne v. Deane*. This case involved a poem, placed on the wall of a private golf club, which was alleged to be defamatory of one of the club's members.[435] Judge Hilbery held that the owners of the club could be held liable as republishers of the defamation.[436] He based this conclusion on the fact that the club owners had complete control of the walls of the club;[437] they had seen the poem;[438] they could have removed it;[439] and yet they did not.[440] In the words of Judge Greer, "by 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."[441]

Courts in this country have made rulings on the posting of defamatory material since at least 1883. *Woodling v. Knickerbocker*[442] involved two placards left on a table at a furniture dealer,

---

[434] *As quoted in* Byrne v. Deane, 1 K.B. 818, 824 (Eng. C.A. 1937).

[435] *Id.* at 818. The case finally held against the plaintiff on the grounds that the message was not defamatory. *Id.*

[436] *Id.* at 820.

[437] *Id.* at 821.

[438] *Id.* at 838.

[439] *Id.*

[440] *Id.*

[441] *Id.*

[442] Woodling v. Knickerbocker, 17 N.W. 387 (Minn. 1883).

one which read, "[t]his was taken from Dr. Woodling as he would not pay for it; for sale at a bargain,"[443] and the other which read, "Moral: Beware of dead-beats."[444] The 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.[445] Importantly, the court also discussed the liability of one of the furniture store owners who had not seen the defamation.[446] 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 of their business.[447] This situation was contrasted with that of a business involved in publishing or selling books or magazines.[448] 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.[449] 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. R. Co.[450] supports this theory. In this case, a newspaper article defaming a ticket broker was posted in the defendant's railway office.[451] 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.[452] Also, by not having it removed 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.[453]

Hellar v. Bianco is a case in which the proprietor of an establish-

---

[443] *Id.*
[444] *Id.*
[445] *Id.*
[446] *Id.*
[447] *Id.*
[448] *Id.*
[449] *Id.*
[450] Fogg v. Boston & L. R. Co., 20 N.E. 109 (Mass. 1889).
[451] *Id.*
[452] *Id.* at 110.
[453] *Id.*

ment 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.[454] *Hellar* involved "libelous matter indicating that appellant was an unchaste woman who indulged in illicit amatory ventures"[455] which was scrawled on a men's room wall of a tavern.[456] 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.[457] Later that evening, when it was not removed, the tavern owner was charged with republication of the libel.[458] The court held that republication occurred when the bartender knew of the libel, and had an opportunity to remove it, but did not do so.[459] In this set of 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.*[460] *Tacket* involved a defamatory sign posted in a GM factory.[461] 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.[462] 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.[463]

A more recent case, *Scott v. Hull*,[464] 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.[465] The plaintiff told the defendant about the graffiti and asked that it be removed; the defendant refused.[466] The court held that the building owners were not liable as republishers, and they were under no duty to remove the graffiti.[467] The reasoning behind this decision is

---

[454] Hellar v. Bianco, 244 P.2d 757 (Cal. Ct. App. 1952).

[455] *Id.* at 758.

[456] *Id.*

[457] *Id.* at 759.

[458] *Id.*

[459] *Id.*

[460] Tacket v. General Motors Corp., 836 F.2d 1042 (7th Cir. 1987).

[461] *Id.* at 1043-34.

[462] *Id.* at 1047.

[463] *Id.*

[464] Scott v. Hull, 259 N.E. 160 (Ohio Ct. App. 1970).

[465] *Id.* at 160.

[466] *Id.* at 161.

[467] *Id.* at 162.

that the viewing of the graffiti was not at the invitation of the owners — as it was in the earlier cases.[468]

In *Scott v. Hull*, the graffiti was on the outside of the defendant's building.[469] It was placed there by strangers and read by strangers.[470] The defamation was not put there by an act of the defendant, and the court refused to find liability for nonfeasance in this instance.[471] In *Hellar*,[472] the defamation was "published" in the restroom on the defendant's premises. The graffiti was placed there by invitees of the defendant,[473] and was read by other invitees.[474] *Byrne v. Deane*,[475] *Woodling v. Knickerbocker*,[476] and *Tacket v. General Motors Corp.*[477] are similar to *Hellar*. The same was true in *Fogg v. Boston & L. R. Co.*,[478] 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 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 as 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 of-

---

[468] *Id.*
[469] *Id.* at 160.
[470] *Id.*
[471] *Id.* at 162.
[472] 244 P.2d at 757.
[473] *Id.*
[474] *Id.*
[475] 1 K.B. at 818.
[476] 17 N.W. at 387.
[477] 836 F.2d at 1042.
[478] 20 N.E. at 109.

fending 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 is 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. These cases all assume that the writing was left by an invitee raising the presumption that the SYSOP is aware of the message, 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.[479] 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."[480] 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.[481] An equal concern is to protect children from inappropriate material; this is especially true because of radio and television's special reach — they can even bring indecent messages to those children too young to read.[482] Radio and television are given special treatment, including the "channeling" of constitu-

---

[479] Communications Act of 1934, 47 U.S.C. § 301.

[480] Red Lion Broadcasting Co. v. F.C.C., 395 U.S. 367, 376 (1969).

[481] *Id.* at 390.

[482] F.C.C. v. Pacifica Foundation, Inc., 438 U.S. 726, *reh'g denied*, 439 U.S. 883 (1978).

tionally 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.[483]

These facts 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.[484]

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 a reduced risk of having the telephone ring and being spontaneously assaulted by a computer spewing lewd data.[485] 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

---

[483] *Id.* at 731.

[484] Action for Children's Television v. F.C.C., 932 F.2d. 1504 (D.C. Cir), *reh'g denied*, 1991 U.S. App. LEXIS 25527, *reh'g denied* 1991 U.S. App. LEXIS 25425 (1991) (en banc).

[485] It is possible for telemarketers to use computers for phone solicitation; it is similarly possible for an individual to prompt a computer to make lewd or obscene phone calls.

guarantees of free speech that apply to publishers apply to broadcasters. For instance, a broadcaster does not have the right to make defamatory statements with knowing or reckless disregard for the truth.[486]

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.[487] Like computer information systems, 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*[488] obscenity standard traditionally was not extended to cable.[489] Recent cable television regulation, however, acknowledges the growth of cable, which now reaches nearly sixty per cent of all television households.[490] The Communications Act of 1934[491] allowed a cable franchising authority to prohibit or restrict any service that "in the judgment 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."[492] 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.[493] 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 re-

---

[486] Adams v. Frontier Broadcasting Co., 555 P.2d 556 (Wyo. 1976).

[487] Mail, 47 U.S.C. § 151; *see also* United States v. Midwest Video Corp., 406 U.S. 649 (1972).

[488] 438 U.S. at 726.

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

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

[491] 47 U.S.C. § 532(h).

[492] Cable Television Consumer Protection Act of 1992, §10(a)(2).

[493] *Id.* § 10(b).

quest.[494] Because wired computer networks are more like cable, cable provides a better analogy than broadcasting. In fact, as mentioned earlier, 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 same need for content restrictions that broadcasters require. While cable television is a better analogy for traditional computer information systems 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.

VIII. SUGGESTIONS FOR REGULATION

Now that the current regulatory environment of computer information systems has been discussed, we are 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[495] and the Electronic Frontier Foundation.[496] 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

---

[494] Id. § 15.

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

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

> 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.[497]

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 incidents like the raid on Steve Jackson Games. This amendment would serve to guarantee that a computer bulletin 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 believes that SYSOPs should be at least jointly liable with the poster of the offending material.[498] 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.[499] Also, it may not even be able to discover the reach of offending material.[500] Copyrighted material could be spread from computer to computer all over the world after just one file transfer.[501]

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 computer crime.[502] 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, tradi-

---

[497] Laurence Tribe Proposed Constitutional Amendment, *available over Internet*, by anonymous FTP, at FTP.EFF.ORG (Electronic Frontier Foundation).

[498] *See generally* Charles, *supra* note 383.

[499] *Id.*

[500] *Id.*

[501] *Id.*

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

tion-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.[503] 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[504] works well to regulate electronic mail because it is modeled after the statute that governs the U.S. mail.[505] 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 difficult 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 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 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.

---

[503] *See* Branscomb, *supra* note 181, at 7-11.

[504] 18 U.S.C. § 2511.

[505] 18 U.S.C. § 1702.