ARTICLES

E-LAW 4: Computer Information Systems Law and System Operator Liability†

*David J. Loundy**

I. Introduction 1076
II. Computer Information Systems Defined 1077
III. Issues Involved 1081
IV. Legal Analogies 1082
  A. Information System as Press 1083
  B. Information System as Republisher/Disseminator . 1087
  C. Information System as Common Carrier 1090
  D. Information System as Traditional Mail 1092
  E. Information System as Traditional Public Forum . 1094
  F. Information System as Traditional Bulletin Board . 1099
  G. Information System as Broadcaster 1102
V. Speech Which Causes Injury 1105
  A. Defamation 1106
  B. Speech Advocating Lawless Action 1115
  C. Fighting Words 1118
  D. "Terrorist" Materials and Hate Speech 1119
VI. Obscene and Indecent Material 1123
  A. Obscenity 1123
  B. Indecent Speech 1126
  C. Child Pornography 1127

---

* Mr. Loundy is an attorney at the law firm of Davis, Mannix & McGrath in Chicago. The author has a J.D. from the University of Iowa College of Law and has a B.A. in Telecommunications from Purdue University. Mr. Loundy is also chairman of the Chicago Bar Association Computer Law Committee, chair of the Internet Law subcommittee of the Illinois State Bar Association Intellectual Property Section Council, and an adjunct professor at the John Marshall Law School. This Article is an updated and revised version of the article *E-Law: Legal Issues Affecting Computer Information Systems and System Operator Liability* which appeared in Volume 3, Number 1, of the *Albany Law Journal of Science and Technology*.

VII. Computer Crime 1131
A. Computer Fraud 1132
B. Traditional Fraud Committed Via Computer Network 1135
C. Unauthorized Use of Communications Services . . . 1136
D. Viruses 1138
E. Protection from Hackers 1140
VIII. Privacy of Electronic Documents 1141
A. Pre-Electronic Communication Privacy Act of 1986 1141
B. Electronic Communications Privacy Act of 1986 . . 1143
C. Access to Stored Communications 1145
D. Privacy Protection Act of 1980 1148
IX. Copyright Issues 1150
A. Basics of Copyrights 1150
B. Copyright and Strict Liability 1155
C. Fair Use On-Line 1157
D. Contributory and Vicarious Infringement 1160
E. Liability for Web Links 1164
F. Copyright Infringement as Wire Fraud 1168
X. Trademark & Unfair Competition Issues 1170
A. Confusion 1170
B. Dilution 1172
C. The Law Applied 1173
XI. Conclusion 1184

I. INTRODUCTION

Cyberspace is the realm of digital data.[1] 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 Lexis 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. It is also the fastest growing communications medium ever invented. 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. Many decisions involving computers and computer networks are fundamentally flawed by a lack of understanding of the technology and how the intricacies of a particular

1. "Computer information systems," as the term is used in this Article, refers to a variety of computer services that, together, make up "Cyberspace."

legal field apply to the particular technology. In some cases decisions are made and legislation is passed with no regard or understanding of what impact there will be on the technology being affected by the legislation or court decision. Only with a proper understanding of both the law and the technology will electronic communications grow unimpeded by the archaic residue of the legal system.

This Article gives a summary of the current regulatory structure in the United States governing a few of the "Empires of Cyberspace," such as bulletin board systems, electronic databases, file servers, networks (such as the Internet) and the like. Different legal analogies that may apply will be illustrated, and some of their strengths, weaknesses, and alternatives will be analyzed. I will begin by looking at different types of computer information systems, and then the major legal issues surrounding computer information systems will be surveyed in brief.[2] Next, the different legal analogies which could be applied to computer information systems will be examined. These different analogies provide an understanding of how courts have seen various communication technologies, and how more traditional technologies are similar to computer information systems. Liability for improper activities—both defining what is improper and who can be held responsible—has been determined by the analogy the courts decide to apply. In the course of this analysis, it will be shown where some judges and legislators have gone wrong. Hopefully, as more attorneys, judges and legislators become familiar with computers and network communication, there will be fewer errors to point out.

II. COMPUTER INFORMATION SYSTEMS DEFINED[3]

As computer communication advances and becomes more commonplace, many services that were once distinct have merged and are harder to distinguish. While once we could talk about bulletin board systems, files servers, chat rooms or channels, etc., systems may now act as all of these services rolled into one entity and accessible at a World Wide Web site. Some of the different technologies are worth distinct examination, however.

A network is a series of computers, connected often by special types of telephone wires. Many networks are conduits used to call up

---

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

3. For more information on specific technologies and terms, a good resource is Requests for Comments (RFCs) and the like put out by the Internet Engineering Task Force. See <http://www.internic.net/ds/dspg0intdoc.html>.

a remote computer in order to make use of that computer's resources from a remote personal computer.[4] Many networks allow a much broader range of uses such as sending e-mail and more interactive forms of communication between machines,[5] transferring computer files, using information distribution protocols such as usenet news and the phenomenally popular World Wide Web (the Web), and also providing the same remote access and use that the simpler networks allow.[6] Networks can be used not only for personal e-mail, but also for a number of special kinds of electronic publishing.[7]

A Bulletin Board System, often referred to simply as a BBS, 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. 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,[8] sometimes directly via a telephone

---

4. Some of the major examples of networks are the Internet—a global network of networks, Sprintnet, and specifically for WESTLAW users there is Westnet.

5. An example of such interactive communication is the UNIX "Talk" command which allows a person to correspond 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. While such uses predated even electronic mail, such services are being replaced by audio and video conferencing technologies which allow users with microphones or video cameras attached to their computers to communicate with other similarly equipped computer users or, in some cases, the computer communications may be interfaced with more traditional telephone networks.

6. An example of these more full-service type networks include the Internet, Bitnet, and ARPANET.

7. One such special use is the electronic mailing list. A message is sent to a "listserver" (sometimes just called a "Listserv") 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 discussion if they do not log on to read their mail regularly. 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. 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.

8. A host computer is the computer that runs the bulletin board software and stores the messages left by users of the BBS.

line,[9] more often via a computer network such as the global Internet. By connecting to the BBS, a user can read the notes (also referred to as messages or posts) of other users or type in his or her own messages to be read by other users. These computer bulletin boards are sometimes referred to as "systems" because they often provide additional services or separate "areas" for posting messages related to different topics.[10] Others may be simple message areas, yet others may be "web-boards" which run on a World Wide Web page and allow the additional hyperlinking or features that the Web protocol[11] allows.

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 or Internet usenet newsgroup[12] to cater to it. Like any communications forum, these discussion forums can raise some serious First Amendment and liability concerns over some of the potential uses, such as availability of pornographic material, defamation, etc.

Another use for networked computers (or bulletin board systems and other services which allow multiple users to connect to the system) is the sending of electronic mail, or e-mail, as it is often called. Electronic mail is a message that is sent from one computer user to another, transmitting either between users on the same computer, or between users on different computers connected together by a network.

---

9. 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.

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

11. The World Wide Web works based on the hypertext transfer protocol (http). Thus any Internet address that begins "http://" indicates that it is a web address. Web pages are written in a special language, Hypertext Markup Language (HTML), which describes how the web page should be displayed by web browsing software. (It is important to note, however, that HTML only roughly describes the look of a web page, some aspects of a web page's appearance are affected by the settings of a specific user's web browser—for instance, the coding of a web page may indicate that some text is emphasized, but the user can determine how text that is emphasized is displayed by his or her web browser).

12. Usenet news is similar to a BBS in practice, but it is a worldwide conferencing system with no central host computer. A user "posts" a message to a particular newsgroup via a service provider's "news server." The news server then passes the message to other news servers from which the first news server receives or gives a "news feed." These receiving news servers then pass the message on to other news servers to which they are connected. The process continues until the posted message achieves worldwide distribution. Local Internet providers who make available usenet news often receive thousands of individual topic-segregated discussion forums.

E-mail and regular mail are different in three important ways. First, because e-mail is provided by private parties, it is not subject to government control under the postal laws as is regular mail.[13] However, it is under the control of the system operator (often called the SYSOP) of the computer system on which it resides at any particular time. 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 of the message. 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. Third, e-mail is interactive in nature and can involve almost instantaneous communication, more like a telephone than regular mail, so much so that regular users of e-mail often refer to the U.S. mail as "snail mail."

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 or network) at the same time. Some of these bulletin boards take the form of slow discussions where messages may be few and may be stored on the system for a long time; others may take the form of a "chat room" or "channel" or "instant messages" where discussions move in near real time,[14] and the messages may not be accessible for long after they are entered by users.

Another service available over computer networks (or many bulletin board systems) is the ability to upload and download files.[15] A computer system providing a file archive, or "file server,"[16] may allow its users to download almost any type of computer file. This may consist of text, software, pictures, sounds, and more. These servers may be seamlessly integrated with other technologies and distribution mechanisms—for instance, a web page may have "links" to software packages which are distributed via a "web server."[17]

---

13. Robert W. Kastenmeier et al., *Communications Privacy: A Legislative Perspective*, 1989 WIS. L. REV. 715, 727 n.75 (1989).

14. In real time conversations, the messages are received at about the same time that they are sent, as opposed to messages which are sent but not received until some time later, such as when the recipient does not actively check to see if any new messages have been posted to a bulletin board.

15. Downloading entails transferring files from the computer on which the files are stored to the user's computer, and uploading is the reverse.

16. A file server (or just "server") is a storage device, such as a disk drive or CD ROM, hooked up to a computer network that lets any computer connected to it access the files contained on the server.

17. Discussed *infra* Part IX.E.

Another common type of information distribution system is the database.[18] These services allow the user to enter a variety of "search terms" to look through the information the service has collected.

Other network based information distribution services include the menu driven "gopher" server (basically, a type of file server), Wide Area Information Server (WAIS),[19] and the Web.

The Web, the fastest growing Internet service, is another method of accessing material on a computer network. Technically, the Web is a protocol—a format for transmitting information over a network, just as e-mail or usenet news are also protocols that distribute information over a network such as the Internet. The Web features the ability to display graphics, sounds, movies, and more. Most importantly though, it allows for hypertext links. Hypertext links are, for example, terms in a document that when selected, call up other documents, (or sounds, pictures, or other materials) which are related to the selected term. From these related documents, links can be followed to yet more related documents, and so on.

III. 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.[20] Just as networked computer systems can be used for political debate, they can also be used as an outlet for defamation. How should they be treated? Who is liable? Is it the user who originally posted the defamation or the system operator who controls and provides the forum?

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. Legal issues arise when these transfers contain copyrighted material. A harder question is who should be liable when data transfers constitute copyright infringement—the transmitter? The

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

19. This is a natural language search system for searching through diverse forms of information stored in a large database or across computer networks—in essence, a large database.

20. For example, defamatory content can be sent via e-mail, cable, traditional broadcasting, or it can even be chiseled into stone tablets. Just as someone can break into a computer system, there has been unauthorized reception of cable and satellite TV signals and cellular phone fraud.

system operator of the machine through which the material passes? The recipient who may have initiated the transfer?

A continual threat to computer users is the computer virus.[21] 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.

Information privacy is another issue for users and operators of computer information systems. With society becoming increasingly computerized, people need to be made aware of the extent to which their stored data and electronic software are secure. 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.[22]

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.

Furthermore, when activities do occur that violate the law, where does one seek redress? When a network such as the Internet is accessible worldwide, and thus difficult to identify from where objectionable material is originating, jurisdiction becomes a complex question.

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.

IV. LEGAL ANALOGIES

Some services allow one entity to deliver its message to a large number of receivers. In this regard, the entity acts like a publisher. Many publishers use web pages to supplement their printed editions

---

21. A virus is a program which replicates itself and moves from computer to computer system by incorporating itself into other programs that are then shared among computer systems. Not all viruses cause damage, though many do. For more information on viruses and related programs, see <http://www.cis.ohio-state.edu/hypertext/bngusenet/comp/virus/top.html>.

22. U.S. CONST. amend. IV.

either by providing additional stories or by providing information services on-line. Some services are nearly indistinguishable from broadcasting. Perhaps an information system operator may literally be a broadcaster because computer services can be provided by sending data over the airwaves. However, other computer services function more like common carriers than publishers. Networks just pass data from one computer to another—they do not gather and edit data. In most cases though, the analogy is that information dissemination may be in the one-to-many form that broadcasters traditionally use. Computer services can also be used to allow many entities to deliver their messages simultaneously to many other entities in a public debate-style setting. 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 is 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 bulletin boards, e-mail, a chat feature, and a file server, one analogy is insufficient. Even the terminology used to discuss a situation can color how it is viewed—*e.g.*, "I visited your web site" versus "you distributed your material into my jurisdiction via your web site." To regulate networked computer systems properly, lawyers, judges, and juries need to understand computer information systems and how they work and when some of these analogies do not cleanly apply.

Liability for illegal activities on-line is affected by how the particular computer information service is viewed. As cases arise around computer communication services, the law applying to old models of communication is looked to for guidance. Therefore, until a distinct body of law evolves to define the limits of liability in a computer network context, it is important to understand how the law affecting other media may apply.

A. *Information System as 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, printed periodicals in essence exist as electronic journals prior to printing.

Even bulletin board operators sometimes see themselves as being analogous to print publishers.[23] Prodigy, a large on-line service provider, is an example of a service that initially saw itself as a publisher. In fact, Prodigy at one point referred to the people who screen messages posted in their conferences as "editors" and not censors, and Prodigy claimed all of them had journalism backgrounds.[24] Both Prodigy and the local newspaper took "articles" by "authors" and "publish[ed]" them in their respective media for the consumption of their "subscribers."

Generally, there are two types of publishers—primary and secondary. A primary publisher is presumed to play a part in the creative process of crafting the message which is then disseminated.[25] Primary publishers are what one generally thinks of when thinking of publishers. Prodigy has claimed to be such a publisher.[26] While the Constitution provides some protection to the editor's judgment as to what to print,[27] the protection is not complete. 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? Defamation[28] generally requires the publisher to have published the defamation with knowing or reckless disregard for the truth.[29] For a SYSOP, at least a "know or have reason to know" standard would be necessary. A SYSOP for a large computer 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. Add in gigabytes of usenet news traffic that typically passes through the average Internet service provider's system, and the amount of content for which there may be liability becomes tremen-

---

23. However, a Wisconsin court has held that a traditional BBS is not, for the purposes of a state defamation-retraction law, a "periodical." It's In the Cards, Inc. v. Fuschetto, No. 94-3162 (Wis. Ct. App., Apr. 11), *rev'd*, 535 N.W.2d 11 (1995). *Compare*, Stern v. Delphi Internet Services Corp., 626 N.Y.S.2d 694, 697 (N.Y. Supp. 1995) which found that for the purposes of a New York invasion of privacy law, an on-line service is analogous to a news disseminator/distributor such as a television network, news vendor, bookstore, or library.

24. 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).

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

26. *See generally*, Stratton Oakmont v. Prodigy Services Co., No. 31063/94, 1995 WL 323710, at *1 (N.Y. Sup. May 24, 1995).

27. U.S. CONST. amend. I.

28. Discussed *infra* Part V.A.

29. New York Times Co. v. Sullivan, 376 U.S. 254, 280 (1964).

dous. While a SYSOP may have the same editorial control that a print publisher has, the sheer volume may effectively prohibit actual editorial control over what is being published over the computer system.

An argument for a "know or reason to know" standard is supported by some cases—for example, those that 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.[30] 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.'[31]

The converse of the position taken in *Yuhas v. Mudge* also supports this "know or reason to know" standard. In *Braun v. Soldier of Fortune Magazine, Inc.*,[32] a magazine was held liable for the results of running a personal services advertisement for, what turned out to be, an assassin.[33] The court found the publisher knew of the likelihood that criminal activity would result from an ad such as the one at issue, as many newspaper and magazine articles had linked past *Soldier of Fortune* personal services ads with criminal convictions.[34] The test the court used was "whether the burden on the defendant of adopting adequate precautions is less than the probability of harm from the defendant's unmodified conduct multiplied by the gravity of the injury that might result from the defendant's unmodified conduct."[35] Employing this test, the court held that the proper balance was to hold the publisher liable when "the advertisement on its face would have alerted a reasonably prudent publisher of the clearly identifiable unreasonable risk of harm to the public that the advertisements posed."[36] The court, in accord with *Yuhas v. Mudge*, held that the

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

31. *Id.*

32. 968 F.2d 1110 (11th Cir. 1992), *cert. denied*, 506 U.S. 1071 (1993).

33. The advertisement read: "GUN FOR HIRE: 37 year old professional mercenary desires jobs. Vietnam Veteran. Discrete [sic] and very private. Body guard, courier, and other special skills. All jobs considered. . . ." *Braun*, 968 F.2d at 1112.

34. *Id.* 1112-13.

35. *Id.* at 1115 (citing United States v. Carroll Towing Co., 159 F.2d. 169 (2d Cir. 1947)).

36. *Id.* at 1115.

publisher's First Amendment concerns should be protected by not requiring the publisher to actually investigate the advertisements, and only to impose liability where a reasonably prudent publisher would determine that an ad "on its face" posed "a clearly identifiable unreasonable risk that the offer in the ad is one to commit a serious violent crime."[37]

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 could not avoid monitoring for improper content, knowing such content is present, and then later claim ignorance.

This test was put to use, to some extent, in the *Stratton Oakmont v. Prodigy* case.[38] In this case, Prodigy lost a motion for summary judgment when the court held that Prodigy could be held liable as a primary publisher for defamatory statements made on one of its bulletin boards.[39] The court held that, because Prodigy had a staff of people who monitored its bulletin boards for messages that do not fit Prodigy's content guidelines, because it has software that automatically screens all bulletin board postings, and because it advertised itself as a service that provides an atmosphere free from certain types of content, Prodigy could be held to be exerting the same content control as a publisher, and thus be subject to the same liability as a publisher.[40]

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.[41] 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

---

37. *Id.* at 1118 (quoting district court's jury instruction). To point out the difficulty with this test, one of the three Justices dissented because although he agreed with the court's test, he found the particular ad ambiguous. *Id.* at 1122 (Eschbach, J., dissenting).

38. No. 31063/94, 1995 WL 323710 (N.Y. Sup. May 24, 1995). The result in this case has been superceded by statute. *See, e.g.*, Zehran v. American Online, Inc., 129 F.3d 327 (4th Cir. 1997).

39. *Statton Oakmont*, 1995 WL 323710 at *1.

40. *Id.* at *4.

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

for defamation.[42] Secondary publishers are often treated synonymously with republishers which are discussed in the next section.

B. *Information System as Republisher/Disseminator*

A republisher, or disseminator, is defined as someone who "circulates, sells, or otherwise deals in the physical embodiment of the published material."[43] Some computer information systems are like republishers because all that they do is make files or messages available, 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 file stored on the computer system. 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."[44]

The case that first established the immunity from liability for distributors, breaking the common law tradition, was *Smith v. California*.[45] The *Smith* case 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 liability, thus would tend to restrict the public's access to forms of

42. *See* RESTATEMENT (SECOND) OF TORTS § 581 (1989).

43. Eric C. Jensen, *An Electronic Soapbox: Computer Bulletin Boards and the First Amendment*, 39 FED. COM. L.J. 217, 247 (1987).

44. *Charles*, *supra* note 25, at 131.

45. 361 U.S. 147 (1959).

the printed word which the State could not constitutionally suppress directly.[46]

While this case did not determine the degree of liability appropriate for a bookseller, it did find that strict liability was too restrictive.[47] 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.[48] In addition, secondary publishers are not required to investigate the contents of the messages they are delivering in order to avoid liability.[49] *Cubby, Inc. v. CompuServe, Inc.* is a major decision supporting the analogy of the computer information system as a republisher or disseminator of media.[50] CompuServe, another large on-line service provider, contracts out its editorial control of various discussion groups to other companies, who maintain the fora in accordance with CompuServe's general guidelines.[51] The groups maintaining these fora are similar to print publishers—they take articles submitted by users and then publish them, exerting editorial control over the material where necessary. CompuServe functions, 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.[52] CompuServe had no opportunity to review the periodical's contents before it was made available to CompuServe's subscribers. District Judge Leisure found that, because CompuServe had no editorial control over the periodical, and CompuServe did not know or have reason to know of the defamation contained in the periodical, CompuServe was, in essence, "an electronic, for-profit library."[53]

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

---

46. *Id.* at 153-54 (citation omitted).

47. *Id.* at 155.

48. *See* Seton v. American News Co., 133 F. Supp. 591, 593 (N.D. Fla. 1955). *Cf.* Manual Enters., Inc. v. Day, 370 U.S. 478 (1962).

49. *Id.*

50. 776 F. Supp. 135 (S.D.N.Y. 1991).

51. *Id.* at 137.

52. *Id.* at 138.

53. *Id.* at 140.

library, and therefore the same "know or have reason to know" standard should apply.

This view is supported by the *Stratton Oakmont* decision, discussed earlier, which held that when a system operator does take substantial steps to monitor system content, it can be held responsible for not doing an adequate job.[54] Thus *Stratton Oakmont* and *Cubby* seem to establish the two ends of the liability spectrum.

With respect to some types of material, Congress has decided to change the balance of these two cases. As part of the "Communications Decency Act"[55] a "safe-harbor" provision was added to provide some immunity for entities which merely carry content provided by others.[56] As one of the first courts to rely on the provision described the situation,

> Whether wisely or not, [Congress] made the legislative judgment to effectively immunize providers of interactive computer services from civil liability in tort with respect to material disseminated by them but created by others. In recognition of the speed with which information may be disseminated and the near impossibility of regulating information content, Congress decided not to treat providers of interactive computer services like other information providers such as newspapers, magazines or television and radio stations, all of which may be held liable for publishing or distributing obscene or defamatory material written or prepared, by others while Congress could have made a different policy choice, it opted not to hold interactive computer services liable for their failure to edit, withhold or restrict access to offensive material disseminated through their medium.[57]

With this safe-harbor provision, Congress is stating that whatever service providers are, they are not to be treated as republishers of other people's content. In fact, this section would seem to provide immunity even when a system operator sees questionable content on a system and actively decides to leave the content publicly accessible.[58] Further-

54. *Stratton Oakmont*, 1995 WL 323710, at *4.

55. Passed as section 502 of the Telecommunications Act of 1996, Pub. L. No. 104-1-, 110 Stat. 133 (1996) (codified as amended at 47 U.S.C. § 609 (1997)).

56. Section (c) (1) reads "(1) TREATMENT OF PUBLISHER OR SPEAKER—No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1) (1994).

57. Blumenthal v. Drudge, 992 F. Supp. 44, 49 (D.C. Cir. 1998).

58. This interpretation was pointedly noted by Judge Friendly in the *Drudge* opinion:

> Because it has the right to exercise editorial control over those with whom it contracts and whose words it disseminates, it would seem only fair to hold AOL to the liability standards applied to a distributor. But Congress has made a different policy choice by

more, in order to specifically address the unpopular *Stratton-Oakmont* decision, subsection (2) provides:

> (2) CIVIL LIABILITY - No provider or user of an interactive computer service shall be held liable on account of—
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[59]

Specifically excluded from this safe harbor provision are violations of any criminal law, intellectual property laws, communications privacy law, or any state law that is consistent with this section.[60] So far, this safe harbor provision has been used to provide immunity for service providers from claims of negligence in allowing the allegedly careless dissemination of defamatory statements,[61] and for use of a service provider's chat rooms to market child pornography.[62]

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 to support a common carrier model. A common carrier is a service that:

> is [of] a quasi-public character, which arises out of the undertaking 'to carry for all people indifferently . . . .' This does not mean that the particular services offered must practically be available to the entire public; a specialized carrier whose service is of possible use to

---

> providing immunity even where the interactive service provider has an active, even aggressive role in making available content prepared by others. In some sort of tacit quid pro quo arrangement with the service provider community, Congress has conferred immunity from tort liability as an incentive to self-police the Internet for obscenity and other offensive material, even where the self-policing is unsuccessful or not even attempted.

Id. at 51-52 (citations omitted).

59. 47 U.S.C. § 230(c)(2) (West Supp. 1998).

60. 47 U.S.C. § 230(d) (West Supp. 1998).

61. Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997). The *Zeran* court held that although not all state claims are preempted, the particular claim at issue is based on attaching liability for distributing others comments, and thus is explicitly preempted by the safe harbor provision. *Id.* at 334. *See also Drudge*, 992 F. Supp. at 44.

62. Doe v. America Online, Inc., No. CL 97-631 AE, 1997 WL 374223, at *2 (Fla. Cir. Ct. June 26, 1997).

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.[63]

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.

Common carriers have generally been considered secondary publishers,[64] and as such, have traditionally functioned under a reduced standard of liability.[65] That standard is, once again, a "know or have reason to know" standard of liability.[66] This standard has been widely adopted and applied to the electronic communications media from telegraphs[67] to telephones,[68] and even to businesses such as telephone answering services.[69] 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 data as well if they also had to monitor content.[70] 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.[71] 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. Thus, 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 applying the same liability standard to a network as is applied to a common carrier.

Like a common carrier, computer networks carry data from one computer to another with no regard for the information being transferred. Data that is transferred over a computer network often consists of electronic mail, web traffic, or other data passively being forwarded from an account on a sending machine to an account on a

---

63. National Ass'n of Regulatory Util. Commr's v. FCC, 533 F.2d 601, 608 (D.C. Cir. 1976).

64. *E.g.*, Von Meysenburg v. Western Union Tel. Co., 54 F. Supp 100, 101 (S.D. Fla. 1944); Mason v. Western Union Tel. Co., 125 Cal. Rptr. 53, 56 (1975).

65. RESTATEMENT (SECOND) OF TORTS § 612 (1989).

66. *Id.* § 581.

67. Western Union Tel. Co. v. Lesesne, 182 F.2d 135, 137 (4th Cir. 1950); O'Brien v. Western Union Tel. Co., 113 F.2d 539, 542 (1st Cir. 1940); *Von Meysenburg*, 54 F. Supp at 101.

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

69. People v. Lauria, 59 Cal. Rptr. 628 (1967).

70. *Charles*, *supra* note 25, at 143.

71. *Id.* at 123.

receiving machine. The volume may be tremendous, and some of the data, such as private e-mail, may be sensitive information. Support for a "knowing" standard is gained from the Electronic Communications Privacy Act of 1986 which statutorily applies this standard to the interception and use of intercepted e-mail and network communications.[72] 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 occurring, and he or she would then be under an obligation to prevent such a use.

D. *Information System as Traditional Mail*

Since a major use for networked computer 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.[73] U.S. mail, or "snail mail" as it is often called by frequent e-mail users, is governed by a statute which gives "regular" mail the same kind of privacy that the Electronic Communications Privacy Act gives e-mail.[74] 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 opens, secretes, embezzles, or destroys the same . . .[75]

This statute has the same effect as the statutes specifically geared towards electronic communications—it protects both mail in transmission,[76] as well as mail being stored for the recipient.[77] Just as the Electronic Communications Privacy Act protects stored communications in the form of an e-mail recipient's "mail box,"[78] so does the postal service protect a "snail mail" recipient's mail box.[79] U.S. mail recipients have certain protections which e-mail recipients may also create for themselves.

72. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511 (1994).
73. U.S. CONST. art. I, § 8.
74. *See* 18 U.S.C. § 2511(1)(b)(iii) (1994).
75. 18 U.S.C. § 1702 (1994).
76. Compare 18 U.S.C. § 1702 with e-mail, 18 U.S.C. § 2511.
77. Compare 18 U.S.C. § 1702 with 18 U.S.C. § 2511.
78. 18 U.S.C. § 2511.
79. 18 U.S.C. § 1702; *see also* United States Postal Serv. v. Council of Greenburgh Civic Ass'n, 453 U.S. 114 (1981).

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.[80] The reason for this protection from unpleasant U.S. mail—based on notions of trespass[81]—has been applied to e-mail and network communications as well.[82] 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. This method is frequently used to screen out unsolicited commercial e-mail.

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.[83] This protection is something that many wish to circumvent in the e-mail context. Unsolicited commercial e-mail, sometimes referred to as "UCE," "UBE" (unsolicited bulk e-mail), or as "spam,"[84] has been the source of much recent debate due to its growing prevalence. The argument is that "junk e-mail" is more like a "junk-fax" than regular "junk (paper) mail." Receiving communication via fax machines usually entails consuming the recipients fax paper and ink, as well as tying up the recipient's fax machine and telephone line. Thus, junk-faxes amount to sending advertising to a recipient who must pay to receive the advertisement, regardless of whether or not it is wanted. The practice of sending junk-faxes became enough of a problem that they were prohibited by Congress.[85]

E-mail presents an analogous situation to faxes for many people. Unsolicited e-mail must be stored on a service provider's computer. It takes system resources to process this unsolicited e-mail. Furthermore, many recipients must pay for the time they spend connected to

---

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

81. *Id.* at 737.

82. *Cf.*, CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997).

83. *See* Bolger v. Young Drug Prods. Corp., 463 U.S. 60 (1983).

84. Spam was originally the term applied to certain types of excessive usenet news posting, where one message is posted to a number of news groups as an individual message sent to each group, rather than as one message sent with a pointer to it in each news group (known as cross-posting). Often these "spammed" messages dealt with commercial transactions. When these advertisements were later delivered by e-mail the term was carried over and applied to unsolicited commercial e-mail as well.

85. 47 U.S.C. § 227(b)(1)(C) (1986).

a computer service in order to receive this mail. Even time spent deleting the messages unread may cost a user for the connect time necessary to process the e-mail. Even more than commercial faxes, commercial e-mail is paid for almost entirely by the recipient and the recipient's service provider, rather than the commercial entity sending the message. Because of this unbalancing of costs, various efforts are under way to ban unsolicited commercial e-mail.[86]

E. *Information System as Traditional Public Forum*

For centuries, when people had ideas to communicate, they did so in public fora, such as parks, streets and sidewalks, and local town squares. These areas are usually "owned" by the government. In many ways, computer information systems, such as bulletin board systems, mailing lists, and chat rooms, are becoming the new public fora. These are mostly operated by individual citizens and corporations.

The First Amendment[87] (and the Fourteenth Amendment[88]) to the U.S. Constitution prohibits the government from restricting content-based speech, or even expressive conduct because of the ideas expressed.[89] Governments can proscribe speech based on some of its aspects, such as potential for harm caused by obscenity and fighting words, but not on the basis of viewpoint.[90] The government may also impose reasonable time, place, and manner restrictions on speech, as long as they are "justified" and the restrictions do not refer to the content of the regulated speech.[91] The law governing speech restrictions pertaining to state owned fora, or fora with sufficient government entanglement to constitute state action, should follow the principles established by the First Amendment. Three cases have specifically examined this issue in the Internet context. The Supreme Court in *Reno v. A.C.L.U.* gave expansive protection to speech on the Internet as a public forum.[92] The court stated,

> As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that government regulation of the content of speech is more likely to interfere with the free exchange of ideas

86. *See, e.g.*, NEV. REV. STAT. § 41.705 [effective July 1, 1998]; 1998 Wash. Laws ch. 149 (H.B. 2752, 55th Legis. effective July 11, 1998).
87. U.S. CONST. amend. I.
88. U.S. CONST. amend. XIV.
89. *See, e.g.*, R.A.V. v. City of St. Paul, 505 U.S. 377 (1992).
90. *See id.* at 385-86.
91. *Id.* at 386 (quoting Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989)).
92. 117 S. Ct. 2329 (1997).

> than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship.[93]

The Supreme Court also struck down portions of the Communications Decency Act[94] as a grossly unconstitutional attempt to impose a content-based restriction on Internet communication. The Court started with the premises that material may originate from any jurisdiction, and may enter any jurisdiction without the ability to limit distribution.[95] Additionally, there is no way to determine the identity or age of people accessing Internet content in most circumstances.[96] That said, even if one could define what material is "indecent," and thus restricted to adults, one has no idea how to restrict minors from accessing the material. Because the Act imposes a blanket restriction on speech based on its viewpoint, the Court held that a "time, place, and manner" argument for regulation is inappropriate.[97] Further, the pervasiveness and scarcity arguments traditionally applied to broadcasting do not fit with the reality of the Internet and thus are not a basis for regulation.[98] In essence, the Court found no reason to allow for a looser standard when regulating speech on the Internet than in any other traditional public forum. Because the Communications Decency Act was "wholly unprecedented"[99] (as well as being vague and ineffectual), the statute was not allowed to stand as a valid government restriction on speech in a public forum.

Similarly, *Urofsky v. Allen* struck down as unconstitutional a Virginia statute intended to provide "[r]estrictions on State Employees Access to [the] Information Infrastructure."[100] The statute stated that "[e]xcept to the extent required in conjunction with a bonafide, agency approved undertaking, no agency employee shall utilize agency-owned or agency-leased computer equipment to access, download, print or store any information infrastructure files or services having sexually explicit content."[101] The court found that such a statute would burden over 101,000 state employees by restricting them from

93. *Reno*, 117 S. Ct. at 2351.

94. 47 U.S.C. § 223(a) (Supp. 1997).

95. *Reno*, 117 S. Ct. at 2335-36.

96. *Id.*

97. *Id.* at 2342-43.

98. *Id.* at 2343-44.

99. *Id.* at 2347.

100. No. 97-701-A, 1998 U.S. Dist. LEXIS 2139 (E.D. Va. Feb. 26, 1998) at *34 (citing VA. CODE ANN. §§ 2.1.804).

101. VA. CODE ANN. §§ 21-80 (Michie 1998).

researching and discussing sexually explicit topics which may be necessary in their areas of expertise; including such areas as a wide range of academics fields, and employees in the state's Department of Corrections, Social Services, Juvenile Justice, Mental Health, and in the Office of the Attorney General.[102] Additionally, the public would be deprived of the benefit of these employee's expertise.[103] In exchange for such substantial restrictions on First Amendment protected speech, the statute would meet its stated goals of improving workplace efficiency and avoiding hostile work environment claims. However, even with the statute in place, workplaces could still be inefficient thanks to networked computers and nonsexually explicit content and other means of creating hostile work environments would still be available to those so inclined.[104] Because content-natural, less burdensome, and more effective methods of addressing the state's interests are available, the ocurt held that the statute was not an acceptable restriction on the right of state employees.[105]

The third case, *Mainstream Loudoun v. Board of Trustees of the Loudoun County Library*, addressed the use of content-filtering software in public libraries along with an accompanying "Policy on Internet Sexual Harassment."[106] This case also held that the state could not restrict adult access to speech appropriate only for minors.[107] Furthermore, the court held that the filtering software did not work to satisfy the goals of the policy because it did not block objectionable material. However, the software did block acceptable (and constitutionally protected) material that the policy did not intend to prohibit.[108] Interestingly, the court rejected a resources-based argument stating that once a library makes internet access available to patrons, all Internet content becomes instantly accessible. Blocking access to material with filtering software actually increases costs and thus a "we must block inappropriate content to preserve scarce resources for more worthy content" argument fails.[109]

While government-owned, publicly-accessible locations are traditionally places where individuals engage in free speech activity, the same rights generally are not enjoyed on private property. Of

102. *Urofsky*, 1998 U.S. Dist. LEXIS 2139, at *13.
103. *Id.* at *14.
104. *Id.* at *15.
105. *Id.*
106. No. 97-2049-A, 1998 U.S. Dist. LEXIS 4725 (E.D. Va. Apr. 7, 1998).
107. *Id.* at *37-*38.
108. *Id.*
109. *Id.*

particular concern to the system operators of privately run computer systems are the limits imposed on control of speech occurring on private property held open for public use. As was held in *Marsh v. Alabama*, "[o]wnership does not always mean absolute dominion. The more an owner, for his advantage, opens up his property for use by the public in general, the more do his rights become circumscribed by the statutory and constitutional rights of those who use it."[110] In *Marsh*, the Court held that a woman could not be prevented from passing out leaflets in a town shopping district which was freely open to the public.[111] What made this situation unusual was that the town in which the woman wanted to pass out her leaflets (Chickasaw, Alabama) was then owned by the Gulf Shipping Corporation. The court reasoned that, because the privately owned town provided all of the services and facilities that would normally be provided by a publicly owned town-such as streets and sewers and the like, and because the company-owned town was otherwise indistinguishable from any other town, the company must also provide for the First Amendment right of the people who wanted to use the "public" areas in their normal fashion.[112]

Marsh has been interpreted expansively, and has been extended to shopping centers.[113] In the *Logan Valley* case, the Supreme Court held that a shopping mall is just like the business district of a company town—both are open to the community and to those passing through, and both serve the same purpose.[114] The Court held that:

> the State may not delegate the power, through the use of its trespass laws, wholly to exclude those members of the public wishing to exercise their First Amendment rights on the premises in a manner and for a purpose generally consonant with the use to which this property is actually put.[115]

These cases were not all the Supreme Court had to say on the issue, however. In *Lloyd Corp., Ltd. v. Tanner*,[116] another shopping center case, the Supreme Court held that, when there is another outlet for speech to be heard, not on private property, a landowner does not

---

110. 326 U.S. 501, 506 (1946).
111. *Id.* at 508.
112. *Id.* at 506-08.
113. *See* Amalgamated Food Employees Union Local 590 v. Logan Valley Plaza, Inc., 391 U.S. 308, 319 (1968).
114. *Id.* at 317-18.
115. *Id.* at 319-20.
116. 407 U.S. 551 (1972).

need to provide his own private property for the speaker's use.[117] The Court noted that *Marsh* held only that where "private interests were substituting for and performing the customary functions of government, First Amendment freedoms could not be denied where exercised in the customary manner. . . ."[118] This decision was refined yet further in *Hudgens v. N.L.R.B.*,[119] which held that *Marsh* applies only to cases in which privately owned property "has taken on *all* of the attributes of a town, *i.e.*, such as 'residential buildings, streets, a system of sewers, a sewage disposal plant, and a 'business block on which business places are situated.'"[120] The Court held that the only way a speaker's First Amendment rights may trump the property rights of the owner of, say, a shopping center, is if that shopping center is the functional equivalent of an entire town, complete with the above listed services.[121] The *Hudgens* holding reflects the current state of private forum law. However, using a traditional private forum model, with this "functional equivalent of the entire town" standard in place, regardless of the extent to which a communications system takes on the aspects of a "community," and no matter how open the system is, until the Supreme Court fundamentally changes its analysis, a user only has speech rights at the sufferance of the system operator.[122] If a computer information system is the functional equivalent to a town, the user may have greater First Amendment rights, but since private computer information systems do not provide a system of sewers and streets, the system operator retains control over how speech is exercised on his or her system. This is especially likely to be true when the system operator requires a service contract before access to the system is given. In this case, not only is the SYSOP not providing the required sewage treatment plants and residential buildings, but the system is also arguably not even open to the public.

---

117. *See id.* at 566-68

118. *Id.* at 562.

119. 424 U.S. 507 (1976).

120. *Id.* at 516 (quoting *Logan Valley Plaza, Inc.*, 391 U.S. at 330-31 (Black, J., dissenting)).

121. *Id.* at 520-21.

122. It is worth pointing out that individual states can provide greater speech protection than is provided for by the U.S. Constitution. For example, California has a constitutional provision which has been held to permit individuals to exercise free speech and petition rights on the property of privately owned shopping centers to which the public is invited. *See* Pruneyard Shopping Center v. Robins, 447 U.S. 75, 85 (1980); CAL. CONST. art. I, § 2.

This analysis was put to the test in *Cyber Promotions, Inc. v. America Online, Inc.*[123] In this case, Cyber Promotions argued that it had a First Amendment right to send unsolicited commercial e-mail to America Online subscribers, and that America Online should not be allowed to block the e-mail. The court, using a variety of tests,[124] rejected a *Marsh*-like analysis and held that America Online's system is private property, and America Online could rightfully exclude Cyber Promotions' unwanted e-mail.[125] Furthermore, a court addressing the same issue with the same defendant held that not only can an on-line service exclude communications from a certain party, but when that party forces its message into the e-mailboxes of the service provider's customers, such actions may constitute a trespass.[126]

F. *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."[127]

A fairly modern case (1937), which is cited more frequently in this country, is *Byrne v. Deane*.[128] This case involved a poem, placed on the wall of a private golf club, that was alleged to be defamatory of one

123. 948 F. Supp. 436 (E.D. Pa. 1996).

124. The court looked at three possible tests to support Cyber Promotions' argument, and found that none of them were met. First, the court did not find America Online exercised "powers that are traditionally the exclusive prerogative of the state." *Cyber Promotions, Inc.*, 948 F. Supp. at 441 (quoting Blum v. Yaretsky, 457 U.S. 991, 1004-1005 (1982)). Second, the court did not find that America Online "has acted with the help of or in concert with state officials," as required by the test in McKeesport Hosp. v. Accreditation Council for Graduate Med. Educ., 24 F.3d 519, 524 (3d Cir. 1994). *Cyber Promotions, Inc.*, 948 F. Supp. at 444-45. Finally, the court found that the State had not so insinuated itself into such a position of interdependence with America Online that the two must be recognized as joint participants in excluding Cyber Promotions' messages, as would be required by the test the Third U.S. Circuit Court of Appeals enunciated in Krynicky v. Univ. of Pittsburgh, 742 F.2d 94, 98 (3d Cir. 1984). *Id.* at 444-45.

125. *Cyber Promotions, Inc.*, 948 F. Supp. at 447. *See also* CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997).

126. *CompuServe*, 962 F. Supp. at 1024.

127. *Quoted in* Byrne v. Deane, 1 K.B. 818, 824 (Eng. C.A. 1937).

128. 1 K.B. 818 (Eng. C.A. 1937).

of the club's members.[129] Judge Hilbery held that the owners of the club could be held liable as republishers of the defamation.[130] He based this conclusion on the fact that the club owners had complete control of the walls of the club;[131] they had seen the poem;[132] they could have removed it; and yet they did not. 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 would be read by people to whom it would convey such meaning as it had, were taking part in the publication of it."[133]

Courts in the U.S. have made rulings on the posting of defamatory material since at least 1883. *Woodling v. Knickerbocker*[134] involved two placards left on a table at a furniture dealer, one which read, "[t]his was taken from Dr. Woodling as he would not pay for it; for sale at a bargain,"[135] and the other that read, "Moral: Beware of dead-beats."[136] 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.[137] Importantly, the court also discussed the liability of one of the furniture store owners who had not seen the defamation. The court said that she could not be held liable for her partner's nonfeasance in removing the sign because there was no way to imply that she had given him authority to act as a publisher of defamatory material, and this was beyond the scope of their business.[138] This situation was contrasted with that of a business involved in publishing or selling books or magazines. 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.[139] *Fogg v. Boston & L. R. Co.* supports this theory.[140] In

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

130. *Id.* at 820.

131. *Id.* at 821.

132. *Id.* at 838.

133. *Id.*

134. 17 N.W. 387 (Minn. 1883).

135. *Id.*

136. *Id.*

137. *Id.*

138. *Id.*

139. *Id.*

140. 20 N.E. 109 (Mass. 1889).

that case, a newspaper article defaming a ticket broker was posted in the defendant's railway office. The court held that a jury could properly have found that the defendant, by way of its agents, had knowledge of what was posted in its office.[141] 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.[142]

In *Hellar v. Bianco*, the proprietor of an establishment was originally unaware of the defamation, which then raised the issue as to what constituted a reasonable time to remove defamatory posts once a proprietor is made aware of their existence.[143] *Hellar* involved "libelous matter" that was scrawled on the men's room of a tavern, "indicating that appellant was an unchaste woman who indulged in illicit amatory ventures,"[144] which was scrawled on a men's room wall of a tavern. After the woman who was the subject of the note began getting calls about the graffiti, the bartender was asked to have the message removed.[145] Later that evening, when it was not removed, the tavern owner was charged with republication of the libel. The court held that republication occurred when the bartender knew of the libel, and had an opportunity to remove it, but did not do so.[146] 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.*[147] *Tacket* involved a defamatory sign posted in a GM factory.[148] The court held that it was conceivable that it could take three days to remove a sign because of the speed at which large bureaucracies work.[149] The court also said, however, 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.[150]

A more recent case, *Scott v. Hull*,[151] appears, at first glance, to hold in a manner contrary to these earlier cases. In *Scott*, graffiti

---

141. *Id.* at 110.
142. *Id.*
143. 244 P.2d 757 (Cal. App. 1952).
144. *Id.* at 758.
145. *Id.* at 759.
146. *Id.*
147. 836 F.2d 1042 (7th Cir. 1987).
148. *Id.* at 1043-44.
149. *Id.* at 1047.
150. *Id.*
151. 259 N.E.2d 160 (Ohio Ct. App. 1970).

defaming the plaintiff was written on the side of a building.[152] The plaintiff told the defendant about the graffiti and asked that it be removed; the defendant refused.[153] The court held that the building owners were not liable as republishers, and that they were under no duty to remove the graffiti.[154] The reasoning behind this decision is that the viewing of the graffiti was not at the invitation of the owners - as it was in the earlier cases. In *Scott*, the graffiti was on the outside of the defendant's building.[155] It was placed there by strangers and read by strangers. The defamation was not put there by an act of the defendant, and the court refused to find liability for nonfeasance in this instance.[156] In *Hellar*, the defamation was "published" in the restroom on the defendant's premises; the graffiti was placed there by invitees of the defendant and was read by other invitees.[157] Of course, as discussed earlier, in the digital context, a bulletin board operator's liability for defamatory material posted by others has been legislatively reduced, if not removed altogether.[158]

G. *Information System as Broadcaster*

Authority to govern broadcasting is given to the Federal Communications Commission (F.C.C.) under the Communications Act of 1934.[159] 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."[160] 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.[161] 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.[162]

---

152. *Id.* at 160.
153. *Id.* at 161.
154. *Id.* at 162.
155. *Id.* at 160.
156. *Id.* at 162.
157. 244 P.2d at 757. *See also Tacket*, 836 F.2d at 1042; *Woodling*, 17 N.W. at 387; *Byrne*, 1 K.B. at 818.
158. *See* discussion *supra*, Part IV.B, Information System as Republisher/Disseminator.
159. 47 U.S.C. § 301 (1934).
160. Red Lion Broadcasting Co. v. FCC, 395 U.S. 367, 376 (1969).
161. *Id.* at 390.
162. *See* FCC v. Pacifica Foundation, Inc., 438 U.S. 726 (1978).

Radio and television are given special treatment, including the "channeling" of constitutionally protected speech, because:

1. children have access to radios and in many cases are unsupervised by parents;
2. radio receivers are in the home, a place where people's privacy interest is entitled to extra deference;
3. unconsenting adults may tune in a station without any warning that offensive language is being or will be broadcast; and
4. there is a scarcity of spectrum space, the use of which the government must therefore license in the public interest.[163]

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; however, the F.C.C. may not altogether prohibit indecent speech.[164]

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 accessing a networked computer system.[165] For example, indecent material available via computer generally must be actively sought. There is little risk of having the telephone ring and being spontaneously assaulted by a computer spewing lewd data. While computers, like radio receivers, are in the home, it generally takes an active effort to obtain indecent material via computer; the risks of accidental exposure to such material at issue in the broadcasting context are just not present.[166] Finally, although children do have unsupervised access to computers, they also may have some potentially unsupervised access to "dial-a-porn"[167] 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.

As well as channeling indecent speech, the other exceptions and guarantees of free speech that apply to publishers also apply to broadcasters. For instance, a broadcaster does not have the right to

---

163. *Id.* at 731.

164. Action for Children's Television v. FCC, 932 F.2d. 1504 (D.C. Cir 1991).

165. In fact, the Supreme Court has held that the broadcasting analogy is the wrong analogy to apply to the Internet, particularly because these factors are not applicable to the Internet. Reno v. ACLU, 117 S. Ct. 2329, 2343 (1997).

166. *See generally* Reno v. ACLU, 117 S. Ct. 2329 (1997).

167. "Dial-a-porn" refers to sexually suggestive material provided by telephone.

make defamatory statements with knowing or reckless disregard for the truth.[168] One court applied this "know or have reason to know" standard in the context of defamation transmitted over television network's affiliated stations.[169] The court held that even where the stations had the technical ability to check for material that should be censored before broadcast, imposing potential liability for everything transmitted without requiring an intent or knowledge requirement "would force the creation of full time editorial boards at local stations throughout the country which possess sufficient knowledge, legal acumen and access to experts to continually monitor incoming transmissions and exercise on-the-spot discretionary calls or face . . . lawsuits at every turn. That is not realistic."[170]

Cable television and cable audio signals are governed in a similar fashion to regular broadcasting. These services are seen as "ancillary" services to broadcasting, and therefore fall under the F.C.C.'s authority.[171] 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, for instance, the *Pacifica* obscenity standard, outlined in *F.C.C. v. Pacifica Foundation*,[172] traditionally was not extended to cable.[173]

Cable television regulation, however, acknowledges the growth of cable, which now reaches a majority of all television households.[174] The Communications Act of 1934 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."[175] 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

168. *See* Adams v. Frontier Broadcasting Co., 555 P.2d 556 (Wyo. 1976).

169. Auvil v. CBS "60 Minutes," 67 F.3d 816 (9th Cir. 1995), *aff'g* 800 F. Supp. 928, 936 (E.D. Wash. 1992).

170. *Id.* at 931.

171. *See* 47 U.S.C. § 152 (1994); *see also* United States v. Midwest Video Corp., 406 U.S. 649, 664 (1972).

172. 438 U.S. 726 (1978).

173. Community Television, Inc. v. Roy City, 555 F. Supp. 1164 1167 (D. Utah 1982); Cruz v. Ferre, 755 F.2d 1415, 1419 (11th Cir. 1985).

174. Cable Television Consumer Protection and Competition Act of 1992, Pub. L. No. 102-385, § 2(3), 106 Stat. 1460 (1992) (codified at 47 U.S.C. § 609) [hereinafter Cable Act].

175. 47 U.S.C. § 532(h) (1994).

activities or organs in a patently offensive manner as measured by contemporary community standards."[176] Cable operators can also refuse to carry programming containing obscenity, indecency, or nudity on public-access stations[177] and on leased[178] channels.

Thus, this standard taken from *Pacifica* now can be applied to cable television. Furthermore, the 1996 changes to the Communications Act now require that a cable operator fully scramble the audio and video to any "sexually explicit adult programming or other programming that is indecent on any channel of its service primarily dedicated to sexually-oriented programming."[179] The Act also requires a cable operator to block on request the audio and video of any channel to which a customer does not subscribe.[180]

V. SPEECH WHICH CAUSES INJURY

Let us start with a hypothetical situation. The Data Playground is a large, full service Internet-accessible bulletin board system. In the BBS's message system, one of the forums, called the Sewer, is set aside for the users as a place to blow off some steam, and express their anger at whatever bothers them. 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 forums which are meant for rational discussions of serious topics. By providing the Sewer, users who get upset with other users or with life in general can "take their problem to the Sewer." Because she is unsure of any liability for posts in the Sewer which get too heated, she posts a disclaimer, which can be seen the first time a user posts in or reads the Sewer, which states that the SYSOP disclaims all liability for anything that is said in the Sewer. Samantha Sysop reads the posts left in the Sewer, and once in a while posts a message there herself. One day a user, Sam Slammer, leaves the following message in the Sewer:

> From: Sam Slammer
> I am sick and tired of logging onto this damned bulletin board and seeing that damn user Dora Defamed here. She is always here. However, at least if she is here it means that she is not still at home beating her young daughter. In fact, her daughter is too good looking to be stuck with a mother like Dora. She should be stuck

176. *Cable Act*, § 10(a)(2).
177. 47 U.S.C. § 531(e) (1994).
178. 47 U.S.C. § 532(c)(2) (1994).
179. 47 U.S.C. § 641(a) (West Supp. 1998).
180. 47 U.S.C. § 640(a) (West Supp. 1998).

> 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 from which Dora is connected to this BBS, I urge you to go over to her and kill her. Do us all a favor.

This hypothetical post clearly raises a number of issues. In one post there is potentially defamatory speech, speech advocating lawless action, fighting words, and perhaps 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 other electronic publications; file servers and databases can distribute defamatory material; and e-mail and usenet news messages can contain defamatory statements. Defamation can even be distributed in the form of a scanned photograph.[181] But what is defamation, and what risks and obligations does it present to the person posting the message and 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 form and "no respectable authority has ever attempted to justify the distinction on principle."[182] 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. "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."[183]

Slander is publication in a transitory form—speech, for example, is slander.[184] Libel, on the other hand, is embodied in a physical, longer lasting form, or "by any other form of communication that has

---

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

182. RESTATEMENT (SECOND) OF TORTS § 568 cmt. b (1989).

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

184. RESTATEMENT (SECOND) OF TORTS § 568(2) (1989).

the potentially harmful qualities characteristic of written or printed words."[185] 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. Though on the other hand, as frequent users of e-mail often notice, e-mail messages and the like can be composed and sent very quickly and with little thought—much like a hastily spoken comment. Printed words last longer than spoken words 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.[186]

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. Even forms of electronic communication such as "chat rooms," which seem to be more fleeting, may be logged. In essence, a transcript may be recorded and stored for an indefinite time period.

Text on a computer screen shares more traits with libel than with slander. Computer text appears as printed words, and it is often more premeditated than spoken words. Computer text can be called from a disk as many times as is needed. The message can even be printed, and the text can be more widely circulated than the same words when they are spoken.

In its barest form, libel is the publication of a false, defamatory, and unprivileged statement to a third person.[187] In other words, there must be a statement that is communicated to another, produces reputational harm to a third party, is untrue, and is made by someone who did not have a socially-accepted reason for making the statement.

"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]."[188] Actual harm to reputation is not necessary for a statement to be defamatory, and the

---

185. *Id.* § 568(1).

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

187. RESTATEMENT (SECOND) OF TORTS § 558 (1989).

188. *Id.* § 559.

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.[189] 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.

"Community" does not refer to the entire community, but rather to a "substantial and respectable minority" of the community.[190] Even more specifically, the community is not necessarily seen as the community at large, but rather as the "relevant" community.[191] 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 arguably 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 potentially reach a larger audience than Sam could have reached by simply posting a notice on a bulletin board affixed to the wall in the local computer center. The remark about child abuse has the potential for lowering people's estimation of Dora, and could easily encourage people to avoid associating with her. Even if people do not avoid Dora because of the remark, in a defamation suit it is sufficient that the statements have the potential to have that effect. 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

---

189. *Id.* § 559 cmt. d.

190. *Id.* § 569 cmt. e.

191. *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. *Id.* at 433.

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.[192]

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.

There is one Australian case which held that speech over a computer "bulletin board" was actionable in a libel suit.[193] This case was a default judgment resulting from messages sent over the DIALx science anthropology computer bulletin board, a discussion group available worldwide and at the time subscribed to by some 23,000 anthropology students and academics. The court found that a number of the statements made were capable of a defamatory meaning; the statements were published throughout academic circles around the world; the statements were likely to be further repeated, gaining in impact in the process; and the statements would have a detrimental impact on the plaintiff's standing in the international academic circles in which his reputation was based.[194] Due to his reputational and psychological injury, the court found that he was deserving of an award of AU$40,000.[195] In our hypothetical case, while the defendant's

192. A person may also be of a different sexual orientation. *See* McVeigh v. Cohen, 983 F. Supp. 215 (D.C. 1998). This case was litigated over the U.S. Navy's attempts to discharge a sailor for homosexual acts in violation of the Navy's "Don't Ask, Don't Tell, Don't Pursue" policy as a result of comments posted on-line in an America On-Line user profile. In his decision, Judge Spoorkin comments that "in the context of cyberspace, a medium of 'virtual reality' that invites fantasy and affords anonymity" comments made on-line may not carry the same weight as comments or observations made in the real world. *Id.* at 219.

193. Rindos v. Hardwick, Supreme Court of Western Australia, unreported, March 31, 1994, 1994/1993, SCLN #940164. *See* <www.law.aukland.ac.nz/cases/rindos.html>.

194. *Id.*

195. *Id.*

note may not have received broad circulation, it is likely that it was read by a substantial and respectable minority of the relevant community.

Because defamation involves speech, serious First Amendment concerns are raised. 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*,[196] which involved an advertisement taken out in a newspaper expressing grievances with the treatment of blacks in Alabama.[197] An elected city commissioner sued, claiming that the statements made in the advertisement defamed him and that the advertisement contained some inaccuracies. Justice Brennan argued that the case should be considered "against the background of a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials."[198]

Because one of the main purposes of the First Amendment was to preserve debate and critical analysis of the affairs of elected officials, the Court held that any censorship of that speech would be detrimental to society.[199] Because of this, the Court said libel laws should be relaxed where the speech pertains to the affairs of elected officials. Likewise, due to the importance of being able to examine the worthiness of public officials, the Court argued that speech critical of officials should also be less open to attack on grounds of falsity. False speech that is made known can be investigated; but true speech that the critic worries may be false, which may result in a libel suit, will remain undisseminated. Because of the importance of monitoring elected officials, the Court held that allowing speech that would aid in the monitoring of elected officials' conduct was more important than protecting officials from potential harm resulting from defamatory speech.

A balance between open debate and freedom from defamation was struck by establishing an "actual malice" standard of liability for the publisher.[200] "Actual malice" is a term of art with a specific meaning in the publishing context. As the Court stated:

196. 376 U.S. 254 (1964).
197. *Sullivan*, 376 U.S. at 256.
198. *Id.* at 270.
199. *Id.* at 279.
200. *Id.* at 279-80.

> 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.[201]

This standard applies to electronic publishing as clearly as it applies to print or speech. Dora, as far as we know, is not a public official. If Dora was merely 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" was 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*,[202] and its companion case, *Associated Press v. Walker*.[203] 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.[204] 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."[205] Because these people have influence in our governance, just as public officials do, the same "actual malice" standard should apply to such public figures.[206] Here, as in the case of public officials, we don't really know who Dora

---

201. *Id.*

202. Curtis Publishing Co. v. Butts, 388 U.S. 130 (1967), *aff'g* 351 F.2d 702 (5th Cir. 1965).

203. Associated Press v. Walker, 388 U.S. 130 (1967), *rev'g* 393 S.W.2d 671 (Tex. Civ. App. 1965).

204. *See Butts*, 388 U.S. at 164 (Warren, C.J., concurring).

205. Gertz v. Robert Welch, Inc., 418 U.S. 323, 342 (1974).

206. *Id.* at 343.

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.*[207] In *Gertz*, a magazine published an article accusing a lawyer of being a "Communist-fronter" and a "Marxist."[208] The article accused the plaintiff of plotting against the police.[209] The plaintiff was a lawyer who played a role in the trial of a police officer who was charged with shooting a boy. 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.*[210] *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.[211] The *Gertz* Court held that this expansion went too far,[212] and the Court overruled *Rosenbloom*.[213]

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.[214] Strict liability would serve to chill the publisher's speech by leading to self censorship where facts are in doubt. This First Amendment interest was balanced against the individual's interest in being compensated for defamatory falsehood.[215] 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 have not voluntarily exposed themselves to the public spotlight.[216] 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."[217]

---

207. 418 U.S. 323 (1974).

208. *Id.* at 326.

209. *Id.*

210. 403 U.S. 29 (1971).

211. *Id.* at 31-32. Matters of public concern have been held to include crackers' "ability . . . to breach the security and threaten the integrity of large computer systems." Wilson v. Slatalla, 970 F. Supp. 405, 413 (E.D. Pa. 1997).

212. *Gertz*, 418 U.S. at 345.

213. *Id.* at 346.

214. *Id.* at 340.

215. *Id.* at 341.

216. *Id.* at 344.

217. *Id.* at 347.

Courts have not made it very difficult for private people to sue for defamation where no matter of public concern is at issue; in one of the more famous defamation cases, *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*,[218] Dun & Bradstreet, Inc. was held liable for a credit report made from inaccurate records contained in a database.[219] The Court argued that statements on matters of no public concern, especially when solely motivated by profit, did not deserve sufficient First Amendment protection to outweigh the individual's interest in suing for defamation.[220]

An interesting issue presents itself in the context of electronic communications when an "access to channels of communication" argument is raised. With access to the Internet readily available even at public libraries, some have argued that everyone has access to the same channels of communication, and thus there should be no difference between public figures and private individuals; everyone should be treated as a public figure.[221] This argument is accurate to the extent that in the Internet age almost anyone in a country with a modern telecommunications infrastructure can have access to an electronic "printing press" capable of reaching millions of people worldwide. However, this does not mean that an individual with an America Online web page can effectively rebut charges made on the New York Times web page. Even though an individual's ability to rebut defamatory statements has increased, so too has the ability to widely distribute the defamatory statements in the first place. The balance of media power may not be realistically any different.

Returning to 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, the ability of one particular company to pay its debts is not necessarily a matter of public concern. Child abuse (which is not an issue in this hypothetical) thus raising the question of "how access to channels of communication" is defined in the on-line context.

---

218. 472 U.S. 749 (1989) (involving a suit for defamation because of a false credit report).

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

220. *Greenmoss Builders, Inc.*, 472 U.S. at 761-62.

221. Mike Godwin, *Libel Law: Let It Die*, WIRED, 4.03, Mar. 1996, at 116.

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,"[222] which is not an issue in our hypothetical. This isolates a reporter from defamatory statements that he or she is reporting.[223] The press is given greater freedom in this area because merely reporting that a certain individual made a certain statement may be a matter of public interest. Therefore, the public interest is best served by allowing the press to inform people that such statements were made, without the imposition of liability upon the reporter.[224] 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.[225] Protection of opinion is, of necessity, not absolute; otherwise "a writer could escape liability . . . simply by using, explicitly or implicitly, the words 'I think.'"[226] Sam Slammer cannot defend himself by saying, "Well, I *think* Dora beats her daughter." The court in *Cianci v. New Times Publishing Co.* 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.[227]

In the hypothetical, Sam made an outright accusation that Dora Defamed committed a criminal act. Even if he had stated that he

---

222. *See* Edwards v. National Audubon Society, Inc., 556 F.2d 113 (2d. Cir. 1977). *See also* Time, Inc. v. Pape, 401 U.S. 279 (1971) (holding that a 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 reprinted a court opinion verbatim was absolutely privileged for any defamatory comments in the court opinion).

223. *Beary*, 763 F.2d at 68.

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

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

226. Cianci v. New York Times Publishing Co., 639 F.2d 54, 64 (2d Cir. 1980).

227. *Id.* (holding that Cianci held the privilege inapplicable to a situation in which the plaintiff was clearly accused of committing a criminal act and distinguishing *Greenbelt Coop. Publishing Ass'n v. Bresler*, 398 U.S. 6 (1970)); Letter Carriers v. Austin, 418 U.S. 264 (1974); Gertz v. Robert Welsh 418 U.S. 323 (1974); Buckley v. Littell, 539 F.2d 882 (2d Cir. 1976); Rinaldi v. Holt, Rinehart & Winston, Inc., 386 N.Y.S.2d 818 (N.Y. App. Div. 1976).

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.

What is Samantha Sysop's liability for the defamatory statements stored on her computer system? As was discussed earlier, as an operator of an "interactive computer service" the "safe-harbor" provision,[228] passed as part of the Communications Decency Act, provides that she is not to be treated as the publisher or speaker of any of Sam's comments. Furthermore, she is not to be held liable for trying to keep her system clear of such objectionable comments, even if she fails in the attempt.[229] Arguably, even if she sees and intentionally leaves the defamatory content publicly available she would not be liable.[230] An individual who posts a defamatory message, on the other hand, would receive no such protection, and would be liable for his or her actions. Unless some sort of privilege exists, or unless it can successfully be argued that the subject of the defamation should have to prove a higher standard to rebut the comments—because of the subject's position in the on-line community or because of the subject's access to the channels of communication—liability should attach to one who posts defamatory comments on-line just as it would in the off-line world.

B. *Speech Advocating Lawless Action*

The First Amendment states that "Congress shall make no law . . . abridging the freedom of speech, or of the press."[231] The First Amendment is one of the most important guarantees in the Bill of Rights, because speech is essential for securing other rights.[232] 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. No matter which standard for examining content is 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.

---

228. 47 U.S.C. § 230(c) (West Supp. 1998).

229. *Id.* at (c) (2).

230. 47 U.S.C. § 230(c); *cf.* Blumenthal v. Drudge, 992 F. Supp. 44 (D.C. Cir. 1998).

231. U.S. CONST. amend. I.

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

One type of speech not permitted is advocacy of lawless action as laid out in *Brandenburg v. Ohio*.[233] The *Brandenburg* Court held that a state may prosecute a person for advocating the use of force or the violation of the law despite the guarantees of free speech and free press "where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action."[234] 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 or in a usenet news group, 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 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 because the incitement may come at a time when action is possible.[235] A chat feature provides nearly instantaneous communication, whereas e-mail or bulletin board postings are not *necessarily* so. While a bulletin board posting may be seen weeks after it was written, and may thus be "stale," a chat feature implies an immediacy which may allow for an imminent incitement in the right factual setting.

One case that created a lot of media attention to the issue of such "lawless" speech on-line is the Jake Baker case.[236] The case involved a college student who posted a story to an Internet news group describing the torture, rape, and murder of a person bearing the name of a fellow student. Further investigation turned up e-mail exchanges

233. 395 U.S. 444 (1969).

234. *Id.* at 447.

235. Regardless of the immediacy of the comments, the "safe-harbor" provision of the Communications Decency Act would seem to isolate Symantha Sysop from liability for the objectionable content. *See* 47 U.S.C. § 230(c).

236. United States v. Baker, 890 F. Supp. 1375 (E.D. Mich. 1995).

with a Canadian man in which they discussed their sexual fantasies involving the kidnapping, torturing, and murdering of women. Furthermore, these e-mail messages discussed specific plans to live out these fantasies. Baker was charged with five counts of violating 18 U.S.C. § 875(c), a sort of statutory offshoot of the imminent lawless action doctrine, which states:

> Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both.[237]

Relying on the decision in *United States v. Kelner*,[238] the *Baker* court argued that the statute could only be constitutionally applied if "the threat on its face and in the circumstances in which it is made is so unequivocal, unconditional, immediate and specific as to the person threatened, as to convey a gravity of purpose and imminent prospect of execution . . ."[239] Furthermore, the court must construe the statements as the receiver (who need not be the object of the threat) is likely to interpret the statements. The court found that the *Kelner* test was not met; the e-mail at issue in the indictment did not sufficiently identify a class of potential victims, and in other cases the actions to be taken were not adequately defined.[240]

While Baker was not convicted under section 875(c), the section was used to convict a college freshman who sent an e-mail message to President Clinton threatening that "One of these days, I'm going to come to Washington and blow your little head off. I have a bunch of guns, I can do it."[241]

In such a case, it is possible that a more adventuresome prosecutor could employ another statute, 18 U.S.C. § 871, which specifically prohibits threats against the President, Vice-President, and certain other officers of the United States:

> (a) Whoever knowingly and willfully deposits for conveyance in the mail or for delivery from any post office or by any letter carrier any letter, paper, writing, print, missive, or document containing any threat to take the life of, to kidnap, or to inflict bodily harm upon

237. 18 U.S.C. § 875(c) (1986).
238. 534 F.2d 1020 (2d Cir. 1976).
239. *Baker*, 890 F. Supp. at 1382.
240. *Id.* at 1387.
241. *In Jail for E-Mail*, WIRED, 2.10, Oct. 1994, at 33.

> the President of the United States . . . shall be fined under this title or imprisoned not more than five years, or both.[242]

If a computer network can be considered "any letter carrier" and an e-mail message "any letter, writing, print, missive, or document," then this statute may be applicable to e-mailed threats as well.

While the *Baker* case involved college students, younger students may have less First Amendment protection for objectional speech. In *Boucher v. School Board of School District of Greenfield*, the court held that a student could be expelled from school for publishing an article providing details for breaking into his school's computer system.[243] The court further held that the student could be punished if the school has "reason to believe" that the student's expression will be disruptive.[244]

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."[245] 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."[246] 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 whether a common person of average intelligence would be provoked into fighting.[247] 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*.[248] Fighting words can be considered delivered to the addressee when the message is read. Dora will become enraged when she reads Sam's

---

242. 18 U.S.C. § 871(a) (West Supp. 1998).
243. 134 F.3d 821, 826-27 (7th Cir. 1998).
244. *Id.* at 827.
245. Chaplinsky v. New Hampshire, 315 U.S. 568 (1942).
246. *Id.* at 572.
247. *Id.* at 573.
248. *Compare Chaplinsky*, 315 U.S. at 573 *with Brandenburg*, 395 U.S. at 446.

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

As with the other types of speech we have discussed, the "safe harbor" provision of the Communications Decency Act would appear to isolate a system operator from liability for threatening speech originating from a user of the system.[249]

D. *"Terrorist" Materials and Hate Speech*

In light of recent terrorist bombings, many people have drawn attention to the availability of hate speech, bomb-making materials, and the like on computer information systems.[250] What these observers do not explain, however, is why it poses less of a threat to have a copy of *The Anarchist Cookbook*,[251] *The Poor Man's James Bond*,[252] or other "mayhem manuals" available in the public library than it does to have the same book available on a computer information system. "Terrorist" materials and hate speech are similar to materials advocating lawless action and fighting words which are both described in the preceding sections.

As mentioned, *Brandenburg* requires that in order to suppress hate speech, the speech must be intended to produce "imminent lawless action" and must be "likely to produce such action."[253] Both elements are necessary. Speech consisting of the "mere *advocacy* of the use of force or violence does not remove speech from the protection of

---

249. 47 U.S.C. § 230(c) (West Supp. 1998).

250. *See, e.g.*, Dennis Romero, *Terrorist Threat Lurking on Info Highway*, CHI. SUN-TIMES, Apr. 24, 1995, at 21.

251. WILLIAM POWELL, THE ANARCHIST COOKBOOK (1971) (book devoted to drug abuse, explosives, and firearms).

252. KURT SAXON, THE POOR MAN'S JAMES BOND (1991) (book devoted to explosives, bombs, and poisons).

253. *Brandenburg*, 395 U.S. at 447.

the First Amendment."[254] As was pointed out in our "Sam Slammer" hypothetical, in the case of a computer bulletin board, messages may not be seen until some time after they are posted. The messages are likely to be read by people who are at home sitting in front of their computers, instead of being heard while rallying outside of the monster's castle, pitchforks and torches in hand. In such a situation the *Brandenburg* test requiring that listeners be incited to immediate lawless action is not as likely to be met.

Hate speech that is sent to inflame the victim of the speech may not be protected under the First Amendment if the speech can be classified as being "fighting words." As discussed above, fighting words are defined by *Chaplinsky* as words that have a direct tendency to provoke acts of violence from the individual to whom the remarks are addressed and that would provoke a person of average intelligence into fighting.[255]

Specific acts of terrorism, conducted across a computer information system, may be outlawed without interference from the First Amendment. One example: if terrorists threaten to kidnap or injure others in a message conveyed over a computer information system, and if the message is sent in interstate or foreign commerce, the note may result in a jail sentence of up to five years and/or a fine of up to $1,000.[256] If the threat is made in an attempt to extort money or anything else of value, the penalty increases to a maximum of twenty years in jail and up to a $5,000 fine.[257] If a kidnapping has already taken place, and the electronic communication is in the form of a ransom note, the party transmitting the note may also be subject to up to twenty years in prison and up to $5,000 in fines.[258] If the communication threatens to injure the property or reputation of the addressee, or threatens to accuse the addressee of a crime, and the communication is transmitted with an intent to extort any money or thing of value, the transmitter of the communication could face up to a $500 fine and could be imprisoned for up to two years, or both.[259]

More generally, while some types of dangerous reference materials may be outlawed in the United States, most materials are protected by the Constitution, even if they have the potential to cause harm. One instance when publication of reference materials likely to cause harm

---

254. NAACP v. Claiborne Hardware Co., 458 U.S. 886, 927 (1982).
255. *Chaplinsky*, 315 U.S. at 573.
256. 18 U.S.C. § 875(c) (West Supp. 1998).
257. 18 U.S.C. § 875(b) (West Supp. 1998).
258. 18 U.S.C. § 875(a) (West Supp. 1998).
259. 18 U.S.C. § 875(d) (West Supp. 1998).

was prevented was the case of an article describing how to make a bomb.[260] This holding, however, concerned the publication of details on how to make a hydrogen bomb, in violation of the Atomic Energy Act.[261] The judge in that case distinguished the particular situation from other Supreme Court precedent that even protected the publication of classified information.[262] The distinction the judge drew was based on the immense destructive potential of furthering the development of nuclear weaponry in other countries. The court noted that "a mistake in ruling against the United States could pave the way for thermonuclear annihilation for us all. In that event, our right to life is extinguished and the right to publish becomes moot."[263]

In cases of distributing information that has the potential to cause damage, except at the level of global destruction, many courts have ruled in favor of allowing the speech to be made without restriction. Such cases have involved everything from stunts performed on the "Johnny Carson Show"[264] to demonstrations on the "Mickey Mouse Club."[265] One of the better illustrations of such cases involved a fourteen-year-old boy, who, after reading a Hustler Magazine article entitled "Orgasm of Death," decided to try the described practice of "auto-erotic asphyxia" at home and hung himself in the process.[266] The court held that the publication of the description of techniques likely to cause harm was protected by the First Amendment. The court stated that, even though protecting children is an important social goal, that concern is to be weighed against "the danger that unclear or diminished standards of [F]irst [A]mendment protections may both inhibit the expression of protected ideas by other speakers and constrict the right of the public to receive those ideas."[267] Therefore, mere negligence in publishing material that may cause harm if used for an improper purpose may not result in liability under an incitement theory.[268]

It is important, however, to distinguish advocacy of lawless action from actual aiding and abetting the commission of a crime. Recently,

---

260. United States v. Progressive, 467 F. Supp. 990 (W.D. Wis. 1979).

261. *Id.* at 996. *See* Atomic Energy Act, 42 U.S.C. § 2274(b).

262. *Id.* at 994 (distinguishing New York Times v. United States, 403 U.S. 713 (1971)).

263. *Progressive*, 467 F. Supp. at 996.

264. DePhillipo v. National Broad. Co., 446 A.2d 1036 (R.I. 1982) (boy hanged himself imitating stunt seen on television).

265. Walt Disney Productions v. Shannon, 276 S.E.2d 580 (Ga. 1981) (child's eye put out by a BB while trying to reproduce a sound effect demonstrated on the Mickey Mouse Club).

266. Herceg v. Hustler Magazine, 814 F.2d 1017 (5th Cir. 1987).

267. *Herceg*, 814 F.2d at 1020.

268. *Id.* at 1024.

the U.S. Fourth Circuit Court of Appeals overturned a district court opinion[269] that held that even "how-to" books on committing murder have been held to be constitutionally protected by applying the *Brandenburg* standard.[270] In its decision, the court held:

> in order to prevent the punishment or even the chilling of entirely innocent, lawfully useful speech, the First Amendment may in some contexts stand as a bar to the imposition of liability on the basis of mere foreseeability or knowledge that the information one imparts could be misused for an impermissible purpose. Where it is necessary, such a limitation would meet the quite legitimate, if not compelling, concern of those who publish, broadcast, or distribute to large, undifferentiated audiences, that the exposure to suit under lesser standards would be intolerable. . . . At the same time, it would not relieve from liability those who would, for profit or other motive, intentionally assist and encourage crime and then shamelessly seek refuge in the sanctuary of the First Amendment. . . . [A]t the very least where a speaker—individual or media—acts with the purpose of assisting in the commission of crime, we do not believe that the First Amendment insulates that speaker from responsibility for his actions simply because he may have disseminated his message to a wide audience.[271]

Of course, holdings such as this leave open the question as to when someone is exercising his or her First Amendment right to publish potentially harmful material, and when such actions constitute "shamelessly seek[ing] refuge in the sanctuary of the First Amendment."[272] As attempts at legislation such as the Communications Decency Act (and further attempts at control arising after the Act's rejection by the Supreme Court) show, legislators are likely to continue to push for regulation of "objectionable" content, including the areas of hate speech and the advocacy of violence. Some of these efforts are likely to be challenged in the Supreme Court, and some of these efforts, in essence, will be challenged by national borders. Any country with an Internet connection may be faced with receiving illegal speech originating in another country over which the objecting country has no control.

269. Rice v. Paladin Enterprises, Inc., 940 F. Supp. 836 (D. Md. 1996).
270. Rice v. Paladin Enterprises, Inc., 128 F.3d 233 (4th Cir. 1997).
271. *Id.* at 247.
272. *Id.*

VI. 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). The degree of liability that attaches depends on which legal analogy is applied to computer information systems. Differences in regulation based on medium are a result of differing First Amendment concerns.[273]

A. *Obscenity*

The constitutional definition of "obscenity," as a term of art, was solidified in *Roth v. United States*.[274] The *Roth* definition asks if the material deals with sex in a manner appealing to prurient interests.[275] This standard was further explained in *Miller v. California*, a case that explored the constitutionality of a state statute prohibiting the mailing of unsolicited sexually explicit material.[276] The Court expressed the test for obscenity as:

> whether
> (a) the average person, applying community standards would find that the work, taken as a whole, appeals to the prurient interest,
> (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and
> (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.[277]

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.[278] Each of the *Miller* prongs critically limits the definition of obscenity.[279] Courts generally have been unwilling to find a national standard for obscenity,[280] and have held that a carrier of obscenity

---

273. *See, e.g.*, Reno v. ACLU, 117 S. Ct. 2239 (1997); FCC v. Pacifica Found., 438 U.S. 726 (1978).

274. 354 U.S. 476 (1957).

275. *Id.* at 487.

276. 413 U.S. 15 (1973).

277. *Id.* at 24 (citations omitted).

278. Pope v. Illinois, 481 U.S. 497, 500 (1987) (citing Smith v. U.S., 431 U.S. 291 (1977)).

279. *Reno*, 117 S. Ct. at 2332.

280. One exception is a 1995 case from the United States Air Force Court of Criminal Appeals, which allowed the use of an Air Force-wide military community standard for obscenity in a court martial trial. United States v. Maxwell, 42 M.J. 568 (1995), *rev'd on other grounds*, 45 M.J. 406 (1996). The court recognized the jury instruction allowing a nationwide community standard rather than a standard gauged by members of the airforce community was erroneous, but

must be wary of differences in definition between the states.[281] This has profound implications for computer information systems that have a national reach. It means electronic publishers must not only be aware of one obscenity standard; they must know the obscenity standards of every jurisdiction in which they distribute content. Publishers 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.[282]

The dilemma caused by the patchwork of local standards applied to computer information systems carrying pornographic information that is accessible from anywhere in the world was clearly illustrated in *United States v. Thomas*.[283] This case involved a couple who ran a bulletin board system out of their home in California. They were convicted in a Tennessee court that applied the obscenity test from *Miller v. California*, and thus applied local Memphis community standards.[284] The conviction resulted from a Tennessee postal inspector calling up the California bulletin board system from Tennessee, applying for an account, and then accessing and downloading a variety of "adult" files. He also requested computer files and videotapes that were sent to him by the Thomases via the United Parcel Service (UPS).[285] After receiving the pornographic materials by modem and UPS, the postal worker had the Thomases charged with transporting obscene materials via common carrier (UPS and the telephone company) and with transporting obscene material in interstate commerce.[286]

Although the BBS was located in California, and served predominantly California users, and even though the postal inspector called long-distance to connect, requested an account, and requested the transmission of the computer files, the Thomases were still found guilty of violating federal statutes by delivering materials that were considered obscene on the other side of the continent. The appellate court explicitly refused to create a community standard based on a community of BBS users.[287] The court said that the Thomases knew

---

found no prejudice as the standard used was more lenient. *Id.* at 425.

281. *See* Hamling v. United States, 418 U.S. 87, 104 (1974).

282. *See, e.g.*, *Miller*, 413 U.S. at 36, n.17.

283. 74 F.3d 701, (6th Cir. 1996).

284. *Id.* at 110.

285. *Thomas*, 734 F.3d at 705.

286. *Id.* They were charged with violations of 18 U.S.C. § 1465 among others.

287. *Id.* at 711.

that they had a user in Tennessee and the Thomases allowed that user to access pornographic materials.[288] Therefore, they were subject to the community standards where that user was located.[289]

On the other hand, individual states may be limited in the extent to which they can "export" their state on-line content laws.[290] Because there is no way to control in which states on-line content is either accessed or routed, state restrictions on on-line speech may run afoul of the "Dormant" Commerce Clause of the U.S. Constitution.[291] A local restriction on network content runs the risk of being struck down if it affects activities that occur wholly outside of the regulating state, and if the burdens on commerce unduly exceed any benefits provided by the regulation.[292] Furthermore, it is possible that if other courts follow the analysis used to strike down a New York network obscenity law, then only national regulation will be found capable of surviving a Commerce Clause analysis.[293]

Also, although states can regulate the availability of obscene material, they cannot forbid the mere possession of it in the home.[294] The justification for this is based on privacy.[295] In the now famous words of Justice Marshall in *Stanley v. Georgia*:

> 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 networked computer 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

---

288. *Id.* at 712.

289. *Id.*

290. American Library Ass'n v. Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997). *See also* Dan L. Burk, *Federalism in Cyberspace*, 28 *Conn. L. Rev.* 1095, 1123-34 (1996) for an excellent analysis of the Dormant Commerce Clause issues.

291. *See Burke, supra* note 290, at 1126-27.

292. *Id.*

293. *See id.* at 1134.

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

295. *Id.* at 565.

296. *Id.*

297. *See* Jensen, *supra* note 43, at 235.

is protected from government regulation.[298] However, connecting to a remote computer information system entails moving obscene material in and out of this zone of privacy, and therefore may not be insulated from state legislation.[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 may protect a person's private library,[303] 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 that is not considered obscene may qualify as indecent. In *F.C.C. v. Pacifica Foundation, Inc.*, the Court held that unlike obscene material, indecent speech is protected by the First Amendment, 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] Furthermore, the restrictions the government may place on indecent speech are very limited, especially when indecent material is transmitted via a medium that requires affirmative steps to access the indecent material.[307] This limitation on the ability to restrict access to indecent material has been explicitly applied to distribution of indecent material via the Inter-

298. Note that an exception would be made for child pornography. *See* discussion *infra* Part VI.C.

299. *See* Davis v. Oklahoma, 916 P.2d 251 (Okla. 1996); *cf.*, United States v. Thomas, 74 F.3d 701 (6th Cir. 1996).

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. *Stanley*, 394 U.S. at 565.

304. Paris Adult Theatre I v. Slaton, 413 U.S. 49, 68-69 (1973).

305. 438 U.S. at 726.

306. *Id.* at 732.

307. Sable Communications of Cal., Inc. v. FCC, 492 U.S. 115, 127 (1989).

net.[308] The Supreme Court has held that unlike in the broadcast context, the Internet bandwidth is not a scarce "expressive commodity," and that previous Supreme Court cases "provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium."[309]

While there may be a strong interest in keeping indecent material away from children, restrictions cannot be placed on this material so as to unduly burden adult access to this material.[310] Because the Internet does not (yet) provide any mechanism for establishing the age of users who may gain access to indecent material, any legislation that limits access to indecent material to adults may provide too great a restriction on the right of adults to access this material via computer network.[311]

As was found in the case of a New York law designed to restrict indecent or obscene material, regulation by individual states of indecent material may be especially problematic.[312] Because of the inability to regulate which jurisdictions Internet traffic passes through, and because of the inability to ascertain from which jurisdictions material published on the Internet may be accessed, state regulation of indecent content may violate principles of federalism in violation of the Commerce Clause of the U.S. Constitution.[313]

C. *Child Pornography*

Another area of content regulated on computer information systems is child pornography. *New York v. Ferber* held that states can prohibit the depiction of minors engaged in sexual conduct.[314] 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.[315] Second, application of the *Miller* standard for obscenity is not a satisfactory solution to the

---

308. *Reno*, 117 S. Ct. at 2343; Mainstream Loudoun v. Board of Trustees of the Loudoun County Library, No. 97-2049-A, 1998 U.S. Dist. LEXIS 4725 (E.D. Va. Apr. 7, 1998); Urofsky v. Allen, No. 97-701-A, 1998 U.S. Dist. LEXIS 2139 (E.D. Va. Feb. 26, 1998).

309. *Reno*, 117 S. Ct. at 2343.

310. *See id.* at 2345.

311. *Id.*

312. *See Pataki*, 969 F. Supp. at 169.

313. *Id.* at 173-74.

314. 458 U.S. 747 (1982).

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

problem of child pornography.[316] 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.[317] Fourth, the value of permitting minors to perform/appear in lewd exhibitions is negligible at best.[318] Finally, classifying child pornography as a form of expression outside the protection of the First Amendment is not incompatible with earlier Court decisions.[319] The Court said, "[T]he distribution of photographs and films depicting sexual activity by juveniles is intrinsically related to the sexual abuse of children . . ."[320] 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.[321] Section 2252 of title 18 of the United States Code forbids knowing foreign or interstate transportation or reception by any means including, for example, visual depictions of minors engaged in sexually explicit conduct, that has been converted into a computer-readable form.[322] The act of sending child-pornographic pictures via computer network to solicit sex has also been held sufficient justification for increasing a pedophile's sentence.[323] Investigations into illegal child-pornography distribution via computer network have resulted in a number of convictions[324] due to child pornography trafficking on America OnLine.[325]

Pictures are easily converted into a computer-readable form. Once in such a form, they can be distributed interstate or internationally over a computer information system. Pictures are put into a computer by a process called "scanning" or "digitizing."[326] Scanning is accomplished by dividing a picture up into little tiny elements called pixels. The equivalent can be seen by looking very closely at a television screen or at a photograph printed in a newspaper. The computer

316. Farber, 158 U.S. at 759 (citing Miller v. California, 413 U.S. 15 (1973)).

317. *Id.* at 761.

318. *Id.* at 762.

319. *Id.* at 763.

320. *Id.* at 759.

321. *See* 18 U.S.C. § 2252 (1978).

322. *Id.* § 2252(a)(1).

323. United States v. Delmarle, 99 F.3d 80, 84 (2d Cir. 1996).

324. *See U.S. Customs Closes Network Transmitting Pornography*, GLOBAL TELECOM REPORT, Mar. 22, 1993.

325. *See, e.g.*, United States v. Black, 116 F.3d 198 (7th Cir. 1997); United States v. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997); United States v. Reinhart 975 F. Supp. 834 (W.D. La. 1997).

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

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.[327]

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, on a web page or through e-mail just like any other computer file.[328] 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 among subject matter of pictures, the law does. Persons responsible for distributing child pornography could be prosecuted, and such a suit could result in $50,000 or more in fines and damages.[329] It has specifically been held that distributing images stored in digital form constitutes "visual depictions" that may form the basis of a child pornography conviction.[330] 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 pornography trafficking.

Another issue raised by Title 18, section 2252, of the United States Code 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

327. *Id.*

328. An interesting issue which may eventually find its way to the Supreme Court is the issue of synthetic child pornography—child pornography that is created on a computer without involving children. The Child Pornography Prevention Act of 1996, 18 § U.S.C. 2252A, outlaws images that even appear to be of a minor engaged in sexually explicit conduct, ignoring the comment made by the Supreme Court in *New York v. Ferber* that simulated child pornography that did not actually use children may have some constitutional protection. *See* New York v. Ferber, 458 U.S. 747, 753 (1982).

Two distinct court cases have examined the constitutionality of the Child Pornography Protection Act of 1996 and have reached opposite conclusions. In the *Free Speech Coalition v. Reno*, No. C-97-0281, 1997 WL 487758 (N.D. Cal. Aug. 12, 1997) Judge Samuel Conti upheld the Act as constitutional. However, in *United States v. Hilton*, No. 97-78-P-C, 1998 WL 167255 (W.D. Me. Mar. 30, 1998) Judge Gene Carter ruled that the Act is unconstitutionally vague.

329. *See* 18 U.S.C. § 2255(a) (1986).

330. United States v. Hockings, 129 F.3d 1069 (9th Cir. 1997).

transported in interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by means including computer"[331] can be fined and imprisoned for up to five years.[332] While the requirement of knowledge may insulate some computer information systems such as networks, it clearly does not protect computer users who knowingly traffic in pornographic material stored in computer files.[333]

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 backups of the computer data that 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 that are no longer in his actual account.[334]

Based on U.S. 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 and that could still be recovered from the system operator's backups of Sam's data. However, if such a claim were to be attempted, it would also need to be shown that Sam knew of the accessibility of these

---

331. 18 U.S.C. § 2252(a)(4)(B).

332. 18 U.S.C. § 2252(b) (1978).

333. United States v. X-Citement Video, Inc., 513 U.S. 64, 68-69 (1994) (holding that the "knowing" requirement of the statute applies to each of the statutory elements that criminalizes conduct that would otherwise be innocent conduct, even if reading the statute to produce this interpretation is not the most grammatical reading of the statute).

334. *Cf.* U.S. v. Lacy, 119 F.3d 742 (9th Cir. 1997). This case held that a defendant must know that images were present on his computer's hard drive to be liable for possession of the images. *Id.* at 748. However, the court also held that it was harmless error to improperly instruct the jury as to the knowledge requirement when the defendant, a computer analyst, claimed to have deleted the pornographic computer files, yet copies were still found on his computer's disks along with other strong evidence that the defendant had knowledge and possession of the illegal pictures. *Id.* at 749.

backups, because the statute requires the *knowing* possession of the pictures.[335] 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 on Samantha's computer system, which she is responsible for maintaining in a legal manner.

VII. COMPUTER CRIME

Computer crime is an ever-present area of concern for operators of networked computer systems. Operators continuously find themselves needing to devote substantial resources to avoid falling victim to system-crackers and the like. The term "computer crime" covers a variety of offenses, including: unauthorized access to and use of computer resources, data theft, damaging stored data, engaging in service attacks, trafficking in stolen passwords, spreading computer viruses, and a number of other related offenses.[336] All of these activities are often referred to as "hacking."[337]

---

335. 18 U.S.C. § 2252(a)(4)(B) (1978). The knowing transportation in interstate commerce element is not difficult to meet—one court has stated that "[t]ransmission of photographs by means of the Internet is tantamount to moving photographs across state lines and thus constitutes transportation in interstate commerce." United States v. Carroll, 105 F.3d 740, 742 (1st Cir. 1997).

336. There are various definitions of "computer crime." *See, e.g.*, Note, *Addressing the New Hazards of the High Technology Workplace*, 104 HARV. L. REV. 1898 (1991), where the author notes that the Office of Technology Assessment defines a "computer crime" as one "in which computerized data or software play a major role," and notes that the Department of Justice defines a "computer crime" as one when "any illegal act for which knowledge of computer technology is essential for successful prosecution." *Id.* at 1898, *citing* OFFICE OF TECHNOLOGY ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: MANAGEMENT, SECURITY AND CONGRESSIONAL OVERSIGHT 85, 86 (1986).

337. Purists argue that the term "cracking" should be used where a destructive intent is present, while "hacking" should be used in the exploratory sense. For the sake of convenience only, the more familiar term "hacking" will be used here to refer to both types of activities.

A. 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.[338]

> [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.[339]

Obtaining information via unauthorized access from the financial records of a financial institution or from a credit reporting agency's consumer file was also outlawed by the act.[340] Accessing a computer 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) were also made illegal.[341]

The 1984 Act was revised by The Computer Fraud and Abuse Act of 1986.[342] The 1986 Act added three new crimes: a computer fraud offense,[343] modeled after federal mail and wire fraud statutes; an offense for the alteration, damage, or destruction of information contained in a "federal interest computer";[344] and an offense for trafficking in computer passwords under some circumstances.[345] Even the knowing and intentional possession of a specified amount of counterfeit or unauthorized "access devices" was made illegal.[346] The 1986 statute has been interpreted to cover computer passwords "which may be used to access computers to wrongfully obtain things of value, such as telephone and credit card services."[347]

---

338. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, ch. 21, 98 Stat. 2190 (codified as amended at 18 U.S.C. § 1030 (1994); 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).

339. Griffith, *supra* note 338, at 460.

340. 18 U.S.C. § 1030(a)(2) (1994); *see also* Griffith, *supra* note 338, at 460.

341. 18 U.S.C. § 1030(a)(2) (1994); *see also* Griffith, *supra* note 338, at 460-61.

342. The Computer Fraud and Abuse Act of 1986, codified at 18 U.S.C. § 1030 (1994).

343. 18 U.S.C. § 1030(a)(4) (1994).

344. 18 U.S.C. § 1030(a)(5) (1994).

345. 18 U.S.C. § 1030(a)(6) (1994).

346. 18 U.S.C. § 1030(a)(6) (1994).

347. United States v. Fernandez, No. 92 CR. 563, 1993 WL 88197, at *2 (S.D.N.Y. Mar. 25, 1993).

The Computer Fraud and Abuse Act presents a powerful weapon for SYSOPs whose computers have been violated by hackers. The first person charged with violating the Act,[348] Robert T. Morris Jr., was charged with releasing a "worm" onto a section of the Internet computer network,[349] causing numerous government and university computers either to "crash" or to become "catatonic."[350] Morris claims that the purpose of his worm program was to demonstrate security defects and the inadequacies of network security, and not to cause harm.[351] However, due to a small error, the worm program got out of control and caused numerous computers to require maintenance to eliminate the worm at costs ranging from $200 to $53,000 each.[352] District Judge Munson read the Computer Fraud and Abuse Act, as it appeared at the time, largely as defining a strict liability crime. The relevant language applied 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 . . . .[353]

The District Court's interpretation that this language only required the intent to access the computer, not an intent to cause actual damage, was affirmed on appeal.[354]

Morris' lawyer, Thomas Guidoboni, described the Computer Fraud Act of 1986 as "perilously vague" because it treats intruders who do not cause any harm just as severely as computer terrorists.[355]

The jury in the *Morris* case indicated that the most difficult question was whether Morris' access to the Internet was unauthorized because, as defense counsel pointed out, two million subscribers had the same access.[356]

---

348. *See* United States v. Morris, 928 F.2d 504 (2d Cir. 1991).

349. *Id.* at 506; 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.

350. *Morris*, 928 F.2d at 506.

351. *Id.* at 504.

352. *Id.* at 506.

353. *Id.* at 506, *citing* 18 U.S.C. § 1030(a)(5)(A) (1994).

354. *Morris*, 928 F.2d at 507-09.

355. 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.

356. 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

This section was clarified in the Computer Abuse Amendments of 1994.[357] The section was amended to broaden the scope of the protection offered in section 1030(a)(5)(A) and to close a loophole contained in the earlier version. "[I]ntentionally accesses a Federal interest computer" is no longer used, and instead, the section applies to anyone who "through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or command to a computer or computer system . . . ."[358] As amended, the section now protects not only federal-interest computers, but also covers privately owned computer systems used in interstate commerce or communication, but that may be affected by someone acting through means of a computer located within the same state as the affected computer.[359] The amendments also remove the "access" requirement from the statute. Instead, a specific intent to perform certain acts which may constitute direct or indirect access has been added.[360] Significantly, the revised statute also adds a requirement that there be either a specific intent or reckless disregard as to whether the transmission will cause damage or will withhold or deny the use of a "computer, computer system, network, information, data, or program" in excess of the user's authorization before liability will be found.[361]

Two other changes to the Computer Abuse Amendments Act of 1994 were made. First, a section providing for civil remedies was added[362] and second, there is now specific protection for actions that modify or impair information or computers used in medical examination or treatment.[363]

The civil provisions were first used in *North Texas Preventative Imaging v. Eisenberg*, which held that a "time bomb" inserted into a software update to ensure payment could constitute a violation of the Computer Fraud and Abuse Act.[364]

---

access to some computers but not others, presenting the question of whether Morris' actions amounted to unauthorized access or whether his actions exceeded authorized access. *Morris*, 928 F.2d at 510.

357. Computer Abuse Amendments of 1994, H.R. 3353, 103rd Cong. (1994) (codified at 18 U.S.C. § 1001, 1030 (West Supp. 1998).

358. *Id.*

359. 18 U.S.C. § 1030(e)(2) (1994).

360. 18 U.S.C. § 1030(a)(5) (1994).

361. *See* 18 U.S.C. § 1030 (1994).

362. 18 U.S.C. § 1030(g) (1994).

363. 18 U.S.C. § 1030(e)(8)(B) (1994) (defining term "damages" to include situations in which medical diagnosis of treatment is impaired).

364. No. CV 96-71, 1996 U.S. Dist. LEXIS 19990, at *22-*23. (C.D. CA. Aug. 1996).

Additional changes have been made to the statute since the 1994 amendments, most noticeably in 1996.[365] In addition to renumbering various sections, the 1996 amendments removed the term "federal interest computer" altogether, replacing it with the term "protected computer."[366] The amendments also added an additional offense: the intentional accessing of a protected computer that recklessly causes damage.[367] Additional modifications were also made to the damage causing provisions to account for actions that cause a denial of service,[368] a growing area of computer crime. Thus, someone like Robert Morris, who intentionally lets a worm loose, but is only reckless in causing damage, would likely be found to violate the statute.

B. *Traditional Fraud Committed Via Computer Network*

More traditional types of fraud may also be carried out via computer network. State and federal regulators have recently started taking an active role in cracking down on fraudulent schemes committed via the Internet and on on-line services. The Federal Trade Commission, for instance, has the authority to prevent unfair or deceptive trade practices through the Federal Trade Commission Act[369] and other statutes the agency is charged with enforcing. Under the authority of these statutes, the Agency has taken action against everything from "run of the mill" pyramid scheme operators[370] to bizarre scams involving software that, when downloaded and run, surreptitiously disconnects the user's computer from his or her Internet service provider, and reconnects the user's computer to a Moldovan telephone exchange (that, in actuality, is really reaching a server in Canada, but the call incurs charges as if the user were calling a number in Moldova).[371] In case anyone had much of a doubt,

---

365. Computer Abuse Amendments of 1996, Pub. L. 104-294, § 201 (codified at 18 U.S.C. § 1001, 1030 (West Supp. 1998).

366. Defined in 18 U.S.C. § 1030(e)(2).

367. 18 U.S.C. § 1030(a)(5)(B) (1994).

368. 18 U.S.C. § 1030(e)(8) defines "damage" to include impairing the availability of data, a program, a system, or information.

369. *See* 15 U.S.C. § 41 (1994).

370. *See* Federal Trade Commission v. The Mentor Network, Inc., Civ. No. SACV 96-1104 LHM (EEx), (C.D. Cal. 1997) (stipulated final judgment and order, available on the Internet at <http://www.ftc.gov/os/9703/mentor.htm> (visited March 29, 1998).

371. Federal Trade Commission v. Audiotex Connection, Inc., No. CV-97 0726 (DRH), (E.D.N.Y. 1997) (available on the Internet at <http://www.ftc.gov/os/9711/AdtxamdFCMPord.htm> (visited March 29, 1998); *In re* Byelen Telecom, Ltd.; File No. 972-3128 (available on the Internet at <http://www.ftc.gov/os/9802/beylene.d&0.htm> (visited March 29, 1998).

service providers who surreptitiously reroute telephone calls to foreign countries in order to receive kickbacks from long distance companies can be held liable for the accompanying deception.[372]

Similarly, if someone offers a product on-line, and then does not deliver, that "merchant" may be held liable under state equivalents to the Federal Trade Commission Act.[373] At least one court has held, that existing state antifraud laws are "an excellent weapon in the soon-to-be-expected war on Internet fraud."[374]

Unfortunately, due to the international reach of computer networks not all fraud is easily prevented. International cooperation will be of growing importance. For instance, when an Australian company masqueraded as a U.S. company that handled domain name registrations, the Federal Trade Commission provided an opinion letter about the legality of the Australian company's actions,[375] which could then be used to influence Australian authorities to investigate the issue.

C. *Unauthorized Use of Communications Services*

One of the favorite targets of computer hackers is the telephone company.[376] Telephone systems are susceptible to computer hackers' illegal use. By breaking into the telephone company's computer, hackers can place free long distance calls to other computers, and can get lists of telephone credit card numbers. Trafficking of stolen credit card numbers and other kinds of telecommunications fraud costs long distance carriers over $1 billion annually.[377] 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.[378]

In addition to a variety of other statutes which may clearly provide a remedy against such unauthorized use,[379] it is possible that

---

372. *Id.*

373. *See, e.g.*, People v. Lipsitz, 663 N.Y.S.2d 468 (1997) (finding a magazine vendor who did not deliver promised magazine subscriptions liable for violating various provisions of New York business law).

374. *Lipsitz*, 663 N.Y.S.2d at 476.

375. See letter from David Medine to David M. Graves, Aug. 21, 1997, available on the Internet at <http://www.ftc.gov/os/9708/internic.let.htm> (visited March 29, 1998).

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

377. *Id.*

378. *Id.*

379. People v. Casey, 587 N.E.2d 511 (Ill. App. Ct. 1992) (holding that unauthorized use of telephone access codes violates state statutes prohibiting theft and unauthorized use of computers).

some protection from hackers is to be found in section 1343 of the Wire Fraud Chapter of the U.S. Code.[380] This section prohibits the use of wires, radio or television in order to fraudulently deprive a party of money or property.[381] This statute has been held to include the fraudulent use of telephone services,[382] and has also been applied to the use of computers to alter account information so as to "steal" airline frequent-flyer miles.[383] However, one case that tried to apply the wire fraud statute to free distribution of pirated software found that while such free distribution may be reprehensible, it was not punishable as wire fraud.[384] Also, it has been held that the mere unauthorized "browsing" of information without any further use or disclosure does not amount to wire fraud or computer fraud.[385] More often, the statute relating to fraud in connection with computer access devices[386] is used to address the theft of communications services. This statute has been interpreted to include computer passwords.[387] This statute has been applied even when no customer account is compromised—theft from the service provider is sufficient.[388] Regardless of whether or not a customer's account is accessed, unauthorized service use creates a potential drag on the efficiency of the entire communications system and results in lost opportunity costs to the service provider.[389] Interestingly though, a few cases have found that "theft of service" in the form of unauthorized use of computer time and disk storage do not constitute larceny and the cases hold that the unauthorized use of such services does not constitute the deprivation of a thing of value as required under the larceny statutes.[390]

---

380. 18 U.S.C. § 1343 (1994).

381. *Id.*

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

383. United States v. Mullins, 992 F.2d 1472 (9th Cir. 1993).

384. United States v. LaMacchia, 871 F. Supp. 535, 545 (D. Mass. 1994).

385. United States v. Czubinski, 106 F.3d 1069 (1st Cir. 1997) (holding that IRS employee did not commit wire fraud or computer fraud by reading tax payer records for personal reasons when there was no evidence of any further use or intent to use the confidential information).

386. 18 U.S.C. § 1029 (1994).

387. United States v. Fernandez, No. 92 CR. 563, 1993 WL 88197 (S.D.N.Y. Mar. 25, 1993).

388. United States v. Ashe, 47 F.3d 770 (6th Cir. 1995); *cf.*, United States v. Taylor, 945 F.2d 1050 (8th Cir. 1991).

389. See United States v. Bailey, 41 F.3d 413, 418-19 (9th Cir. 1994), *cert. denied*, 515 U.S. 1134 (1995) when the court discussed the costs of cloning even when a customer account was not compromised. In addition to the Federal statutes, some state laws also exist to punish theft of local telephone service or publication of telephone access codes. *See, e.g.*, State v. Northwest Passage, Inc., 90 Wash. 2d 741, 585 P.2d 794 (Wash. 1978) (en banc).

390. United States v. Collins, 56 F.3d 1416, 1421 (D.C. Cir. 1995); State v. McGraw, 480 N.E.2d 552, 554 (Ind. 1985).

D. Viruses

As pointed out in the introduction, computer viruses are increasingly of concern—both for operators of computer information systems, and 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.[391] Computer virus crime involves an intent to cause damage, "akin to vandalism on a small scale, or terrorism on a grand scale."[392] Viruses can be spread through networked computers or by sharing disks between computers.[393] Viruses cause damage by attacking another file or by simply filling up the computer's memory or by using up the computer's processor power.[394] 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). Viruses are, in essence, self-replicating.[395]

Also discussed earlier was a "pseudo-virus," called a worm.[396] People in the computer industry do not agree on the distinctions between worms and viruses.[397] Regardless of the exact definition, however, a worm is a program specifically designed to move through networks.[398] 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 . . . [that] 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."[399]

Another type of virus is the "Trojan Horse."[400] These are viruses that hide inside another seemingly harmless program. Once

---

391. *See, e.g.*, Daniel J. Kluth, *The Computer Virus Threat: A Survey of Current Criminal Statutes*, 13 HAMLINE L. REV. 297, 297-98 (1990).

392. *Id.* at 298.

393. David R. Johnson, *Computer Viruses: Legal and Policy Issues Facing Colleges and Universities.*, 54 EDUC. L. REP. 761 (1989).

394. *Id.* at 762.

395. *Id.*

396. See *Morris*, 928 F.2d 504 and discussion, *infra* at § VII2A.

397. Eric Allman, *Worming My Way; November 1988 Internet Worm*, UNIX REV., Jan. 1989, at 74.

398. Kluth, *supra* note 391, at 300.

399. *Id.* at n.14.

400. *Id.* at 298.

the Trojan Horse program is used on the computer system, however, the virus spreads.

The virus type that has gained the most fame recently has been the "Time Bomb," which is a delayed action virus of some type.[401] 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.[402] Michelangelo was so prevalent, it was even distributed accidentally by some software publishers when the software developers' computers became infected.[403]

One concern many have about the statutes dealing with computer viruses is the problem of an intent requirement.[404] Without some sort of intent requirement, virus statutes may be so overbroad so as to cover defective computer programs.[405]

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.[406] If a virus also involves unauthorized access to an electronic communications system involving interstate commerce, the Electronic Communications Privacy Act may come into play.[407] Most states have statutes that make it a crime to intentionally interfere with a computer system.[408] These statutes will often cover viruses as well as other forms of computer crime.[409]

SYSOPs must also worry about being liable to their users as a result of viruses that cause a disruption in service.[410] Service outages

---

401. Dawn Stover, *Viruses, Worms, Trojans and Bombs: Computer Infections*, POPULAR SCIENCE, Sept. 1989 at 59.

402. Steve Alexander, *Viruses: Some Are Just Ornery, Some Are Deadly. Here's How to Head 'em off at the Pass*, COMPUTER WORLD, June 2, 1997 at 88.

403. *Electronic Mail Software Provider Reports Virus Contamination*, UPI, Feb. 3, 1992, at 1, *available in* LEXIS, Nexis Library, UPI File.

404. *See* Kluth, *supra* note 391, at 300.

405. *Id.*

406. 18 U.S.C. § 1030 (1994).

407. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 (1994).

408. Johnson, *supra* note 393, at 764. *See also* 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). For direct application of such a state statute, see, People v. Versaggi, 629 N.E.2d 1034 (N.Y. 1994).

409. *See, e.g.*, State v. Corcoran, 522 N.W.2d 226 (Wis. Ct. App. 1994). States may have a wide variety of statutes which can be applied to various activities that involve inappropriate computer use. *See, e.g.*, People v. Krause, 609 N.E.2d 980 (Ill. App. Ct. 1993) (finding a police officer guilty of violating a statute prohibiting official misconduct because he used a computer system to investigate prostitution customers).

410. *See* Johnson, *supra* note 393, at 761.

caused by viruses or by shutdowns to prevent the spreading of viruses could result in a breach of contract when 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, system operators are open to tort suits caused by negligent virus control.[411]

> [A SYSOP] might still be found liable on the ground that, in its role as operator of a computer system or network, it failed to use due care to prevent foreseeable damage, to warn of potential dangers, or to take reasonable steps to limit or control the damage once the dangers were realized.[412]

The nature of "care" has not been defined by court or by statute. 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.

E. *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 negligent failure to secure their computer information system. For a system operator to be found negligent, there must first be a duty of care to the user who is injured by the hacker.[413] There must then be a breach of that duty,[414] i.e., the SYSOP must display conduct "which falls below the standard established by law for the protection of others against unreasonable risk of harm."[415] 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 when foreseen and planned for—will not result in liability.[416] A SYSOP's duty "may be defined as a duty to select and implement security provisions, to monitor their effectiveness, and

---

411. *Id.* at 764, 766.

412. *Id.* at 766.

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

414. *Id.* § 30(2), at 164.

415. *Id.* § 31, at 169.

416. *Id.* § 29, at 162.

to maintain the provisions in accordance with changing security needs."[417] 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 which users are authorized to use what data and services. System operators also have a duty to explain to each user the extent of his or her authorization to use the computer information service.[418]

The same analysis applies to operator-caused problems. If the system operator 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.

VIII. PRIVACY OF ELECTRONIC DOCUMENTS

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.[419] It is imperative that users of services such as electronic mail understand how these services work. They must understand 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. Similarly, it is important that system operators 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*.[420] *Katz* involved the use of an electronic listening device (or "bug") mounted on the outside of a public telephone booth.[421] The government (who placed the bug) assumed that because the bug did not actually penetrate the walls of the booth, and was not a "wire tap," there was no invasion of

---

417. 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).

418. *Id.* at 188-89.

419. For example, the United States Supreme Court noted that "[p]lainly there is a vast difference between the public records that might be found after a dilligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a singular clearinghouse of information." United Stated Dept. of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 764 (1989).

420. 389 U.S. 347 (1967).

421. *Id.* at 348.

privacy.[422] However, the defendant argued that the bug was an unlawful search and seizure in violation of the Fourth Amendment. The Court held:

> the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. [citations omitted] But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[423]

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.[424]

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.[425] For example, most people have a reasonable expectation that calls made from inside a closed telephone booth will be private. For computer users, although the system operator can read the user's e-mail, there may still be an expectation of privacy,[426] especially on a "closed" system such as America Online or CompuServe, as opposed to an Internet transmission. However, this, of course, does not mean that a user may have a right to expect that the recipient of a message on an on-line service will keep the contents of a message secret.[427]

Statutory protection of the right to privacy was originally provided by the Federal Wiretap Statute.[428] However, this statute affected only "wire communication," which was limited to "aural [voice] acquisition."[429] Even if the Act did cover transmission, it still did not cover stored computer data.[430] This does not result in significant or comprehensive protection of e-mail or stored data.

---

422. *Id.* at 351.

423. *Id.*

424. *See, e.g.*, Oliver v. United States 466 U.S. 170 (1984).

425. *See* California v. Ciraolo 476 U.S. 207 (1986).

426. United States v. Maxwell, 42 M.J. 568, 576-77 (1995).

427. *See, e.g.*, United States v. Carbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997).

428. 18 U.S.C. § 2510 (1994).

429. *See* United States v. Seidlitz, 589 F.2d 152, 156-57 (4th Cir. 1978), *cert. denied*, 441 U.S. 922 (1979) (holding that interception of computer transmission is not an "aural acquisition" and, therefore, the Wiretap Act did not provide protection).

430. *Id.* at 157 (discussing fact that the statute did not apply to retrieval of information from computer prior to transmission).

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 Amendment'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.[431]

The Federal Wiretap Act was updated by the Electronic Communications Privacy Act of 1986.[432] The Electronic Communications Privacy Act deals specifically with the interception and disclosure of interstate electronic communications.[433] 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" shall be fined or imprisoned.[434] 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.[435] This largely guarantees the privacy of in-transit e-mail as well as data transfers over a network or telephone line going to or from a computer 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 provides an exception for system operators and their employees to the extent necessary to properly manage the computer system:

---

431. Robert W. Kastenmeier et al., *supra* note 13, at 720 (citations omitted).

432. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 (1994).

433. *Id.* §§ 2510(12), 2511.

434. *Id.* § 2511.

435. *Id.* § 2511(1)(c).

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.[436]

"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."[437] Further exceptions are made for system operators of these systems when the originator or addressee of the message gives consent;[438] when the message is being given to another service provider to be further forwarded towards its destination;[439] where the message is inadvertently obtained by the SYSOP and appears to pertain to a crime;[440] when the divulgence is being made to a law enforcement agency;[441] or where the message is configured so as to be readily accessible to the public.[442] 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).[443] This will probably cover the up-and-coming technologies of radio-WANS,[444] cellular modems, and packet radio. These technologies are especially likely to be covered by the statute if data is transmitted using some sort of encryption scheme.[445]

For law enforcement agencies to intercept electronic communications, they must first obtain a search warrant by following the

---

436. *Id.* § 2511(2)(a)(i).
437. *Id.* § 2510(14).
438. 18 U.S.C. § 2511(3)(b)(ii) (1994).
439. *Id.* § 2511(3)(b)(iii).
440. *Id.* § 2511(3)(b)(iv).
441. *Id.* § 2511(3)(b)(iv).
442. *Id.* § 2511(3)(b)(i).
443. *Id.* § 2511.
444. Radio-WANS are Wide Area Networks, *i.e.*, computer networks which link computers by radio transmissions rather than wires.
445. 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.

procedure laid out in section 2518 of this Act.[446] The statute does not prohibit the use of pen registers or trap and trace devices.[447] The 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 while section 2701 of the Act prohibits unlawful access to communications which are being stored on a computer.[448] E-mail, voice mail, and even pager data are stored at some point during the transmission process.[449] Section 2701 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"[450] shall be subject to fines and/or imprisonment.[451] Like section 2511, section 2701 includes provisions prohibiting the divulgence of stored messages.[452] Importantly, while section 2701 allows law enforcement agencies to gain access to stored communications, it also specifically allows the government to permit a system operator to first make backup copies of stored computer data, subject to a valid search warrant.[453] Section 2701 enables electronic communications to be preserved for use outside of any government investigation.[454]

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*

446. 18 U.S.C. § 2518 (1994).

447. *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.

448. 18 U.S.C. § 2701 (1994).

449. *See*, Thomas R. Greenberg, Comment, *E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U. L. REV. 219, 247-48 (1994).

450. 18 U.S.C. § 2701(a) (1994).

451. *Id.* § 2701(b) (1994).

452. *Id.* § 2702.

453. *Id.* § 2703.

454. *Id.* § 2703(a).

Service (Steve Jackson Games).[455] In that case, the Secret Service raided a publisher and seized its BBS—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 properly the contents of the electronic mail on the BBS.[456] The court indicated that evidence of good faith reliance on a search warrant that the Secret Service believed to be valid was insufficient.[457] 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 compliance with the Electronic Communications Privacy Act, and not by seizing the BBS.[458]

The *Steve Jackson Games, Inc.* case is also valuable in that it demonstrates the interplay between protection against interception of electronic communication and access to stored communication.[459] The district court 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-provided by section 2701 *et seq.* The court analogized the situation to the seizure of a tape recording of a telephone conversation and held that the "aural acquisition" occurs when the tape is made, not each time the tape is played back by the police.[460] This interpretation was appealed on the grounds that, because the messages had been sent and not yet received, they were intercepted, just as if someone had picked up and carried off a postal service mailbox from the side of the street.[461] However, the Fifth Circuit affirmed Judge Sparks' interpretation of the interplay between sections 2701 *et seq.* and 2510 *et seq.* of the Electronic Communications Privacy Act.[462]

However, not all cases have reached the same conclusion as that reached in the *Steve Jackson Games* case as to the legality of seizing a BBS, stored communications and all. In *Davis v. Gracey*, the court held that when officers rely on a valid search warrant and when such reliance is objectively reasonable, the incidental seizure of the electronic communications will not result in liability thanks to the "good faith"

455. 816 F. Supp. 432 (W.D. Tex. 1993), *aff'd*, 36 F.3d 457 (5th Cir. 1994).
456. *Id.* at 443.
457. *Id.*
458. *Id.* at 442-43.
459. *Id.*
460. *Id.* at 441-42.
461. *Steve Jackson Games, Inc.*, 36 F.3d at 457.
462. *Id.*; Wesley College v. Pitts, 974 F. Supp. 375, 386-87 (D. Del. 1997).

exemption from liability provided by section 2707(e) of the Act so long as the seizure of the stored electronic communications was incidental to the execution of the warrant.[463]

Another important limitation to point out is that section 2701 applies to the divulging of communications to which access is not authorized.[464] If access to the stored communication is authorized—because the party accessing the communication is the owner of a private communications system—disclosure of the communication may be allowed.[465] On the other hand, if the communication service is being provided to the public, the service provider is limited in its ability to divulge the contents of stored communication[466] unless one of the permitted exceptions is met.[467]

At this point, it is worth mentioning a case that has drawn criticism because the opinion did not mention the Electronic Communications Privacy Act. *Smyth v. Pillsbury* involved the firing of an at-will employee for sending e-mail to a superior that was judged to be "inappropriate and unprofessional."[468] The employer had previously assured its employees, including the defendant, that all e-mail was privileged and confidential, and would not be used against its employees as grounds for termination or reprimand.[469] In finding that the interception of the employee's e-mail did not constitute a common law tortious invasion of his privacy, the court stated that it did "not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management."[470] Furthermore, the court held that even if the employee did have a reasonable expectation of privacy, the employer's desire to prevent use of the e-mail system for carrying "inappropriate" comments would outweigh any privacy interest that employee may have in those comments.[471]

Another important limitation to point out is that section 2701 applies the divulging of communications to which access is not

463. 111 F.3d 1472, 1481 (10th Cir. 1997).
464. 18 U.S.C. § 2701(a).
465. *See id.*
466. 18 U.S.C. § 2702(a).
467. *Id.* § 2702(b).
468. 914 F. Supp. 97, 98 (E.D. Pa. 1996).
469. *Id.*
470. *Id.* at 101.
471. *Id.*

authorized.[472] If access to the stored communication is athorized, because the party accessing the communication is the owner of a private communications system, disclosure of the communication may be allowed.[473] On the other hand, if the communication service is being provided to the public, the service provider is limited in its ability to divulge the contents of stored communications[474] unless one of the permitted exceptions is met.[475]

D. Privacy Protection Act of 1980

Computer systems also fall under the protection of the Privacy Protection Act of 1980.[476] 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."[477] This statute was passed to overturn the decision in *Zurcher v. Stanford Daily*, a case that held that a newspaper office could be searched, even when no one working at the paper was suspected of a crime.[478] 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,[479] or the immediate seizure is necessary to prevent the death or serious injury to a human being.[480] A computer system may fall under this statute when it is being used in the aid of a print publisher, such as when the service is used in a publisher's office or to transmit materials to a publisher.[481] More importantly for the System Operator, electronic publishers should fall directly under this section based on the list of types of "publishers" covered by this statute.

The first case that attempted to apply this statute to electronic publishers was *Steve Jackson Games*, mentioned earlier. *Steve Jackson*

472. 18 U.S.C. § 2701(a) (1994).
473. *See* Anderson Consulting LLP v. UOP Inc., 991 F. Supp. 1041 (N.D. Ill. 1998).
474. 18 U.S.C. § 2702(a) (1994).
475. *Id.* § 2702(b).
476. Privacy Protection Act of 1980, 42 U.S.C. § 2000aa (1980).
477. *Id.* § 2000aa(a).
478. 436 U.S. 547, 560 (1978).
479. 42 U.S.C. § 2000aa(a)(1) (West Supp. 1998).
480. *Id.* § 2000aa(a)(2) (1994).
481. For example, journalists reporting from a war zone can use a laptop computer and a satellite telephone to transmit an article to an e-mail service, where the article can then be sent to the publisher. *See Electric Word,* WIRED, 1.6, Dec. 1993 at 27.

Games presents 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.[482] The company also ran a BBS to gain customer feedback on the company's games.[483] The Secret Service took all of the company's computers—their regular business computers and the one on which they were running the company's BBS (private electronic mail, etc.).[484] They also took all of the copies of their latest game, "Gurps Cyberpunk."[485] The raid by the Secret Service caused the company to temporarily shut down.[486] Steve Jackson Games also had to lay off several employees.[487] The release of the game was delayed for months, because the Government took all of the word processing disks as well as all of the printed drafts of the game.[488] 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.[489] Steve Jackson Games was raided because one of its employees ran a BBS out of his home—one home one out of several thousand possible homes around the country that distributed the electronic journal "Phrack," in which a stolen telephone company document was published.[490] The document contained information which was publicly available in other forms.[491] The employee was also accused of being a part of a fraud scheme—the "fraud" consisting of an explanation, in a two-line message of "Kermit," which is a publicly available communications protocol.[492] The employee was also co-SYSOP of the bulletin board system at Steve Jackson Games. The court found 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).[493] As a result, the Secret Service did not comply with

482. Steve Jackson Games, Inc. v. United States, 816 F. Supp. 432, 434 (W.D. Tex. 1993) *aff'd*, 36 F.3d 457 (5th Cir. 1994).

483. *Id.*

484. *Id.* at 439.

485. *Id.* at 439-40.

486. *Id.* at 438.

487. *Id.*

488. *Id.*

489. Legal Case Summary, May 10, 1990, available on the Internet by anonymous FTP at FTP.EFF.ORG (Electronic Frontier Foundation) (visited March 29, 1998).

490. *Steve Jackson Games, Inc.*, 816 F. Supp. at 436.

491. *See* United States v. Riggs, 743 F. Supp. 556, 558 (N.D. Ill. 1990).

492. *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) (visited March 29, 1998).

493. *Id.* at 436.

the provisions of the Privacy Protection Act.[494] Judge Sparks said that 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.[495] In the raid, the Secret Service seized a number of Steve Jackson's computers, and a number of papers.[496] 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.[497]

While the judge found a violation of the Privacy Protection Act, he did not specify which items led to the violation. The violation 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 Games were also plaintiffs in the case.[498] They were not allowed recovery based on the Privacy Protection Act.[499] 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.

IX. COPYRIGHT ISSUES

A. *Basics of Copyrights*

Text, pictures, sounds, software—all of these can be distributed via computer systems—and all can be copyrighted. Section 101 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."[500]

The element of fixation is important in the copyright statute; a work that is not fixed is not covered by the statute, and any possible

494. 42 U.S.C. § 2000aa (1994).
495. *Steve Jackson Games, Inc.*, 816 F. Supp. at 437.
496. *Id.*
497. *Id.* at 439-40.
498. *Id.* at 439.
499. *Id.*
500. 17 U.S.C. § 101(a) (1994).

protection must come from local common law.[501] A number of controversial cases have held that reading copyrighted material into a computer's Random Access Memory (RAM) constitutes making a copy (or a fixation).[502] These cases are controversial because a computer's RAM retains information only while the computer is turned on, and requires a constant "refreshing" of the stored information in order to avoid losing the data. Thus, the information stored in a computer's RAM is only temporarily fixed, at best. However, a temporary fixation is all that is required by the Copyright Act for the purposes of finding that a copy has been made.[503] These cases are also controversial because, while the Copyright Act explicitly allows copies of computer programs to be made in the limited circumstance of making an archival copy of the program[504] or a copy necessary to utilize the software (*i.e.* a RAM copy),[505] this section *only* covers computer programs. A computer program is defined in the Copyright Act as "a set of statements or instruction to be used directly or indirectly in a computer in order to bring about a certain result."[506] Arguably data in raw form, such as e-mail and sound and picture files, does not meet the definition of a computer program, and thus may not even be copied into a computer's RAM as is necessary to utilize the data without risking a copyright infringement (unless such a copy fits under one of the exceptions such as the fair use provision).[507] More

---

501. *Id.*

502. MAI Syss. Corp. v. Peak Computer, Inc., 991 F.2d 511 (9th Cir. 1993); Advanced Computer Services of Mich., Inc. v. MAI Syss. Corp., 845 F. Supp. 356 (E.D. Va. 1994); Triad Systems Corp. v. Southeastern Express Co., 31 U.S.P.Q.2d 1239 (N.D. Ca. 1994), *cert. denied*, 516 U.S. 1145 (1996).

503. 17 U.S.C. § 101 (1994) (defines a work to be "fixed" in a tangible means of expression "when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than a transitory duration"). In *Marobie-FL, Inc. v. National Ass'n of Fire Equipment Distributors*, 983 F. Supp. 1167, (N.D. Ill. 1997), a service provider made an interesting argument, that the court, unfortunately, seemed to miss. The service provider argued that it was not liable for copyright infringement because its computers processed the copyrighted work so quickly that at no point was a complete copy of the protected works in the computer's RAM at any one time. *Id.* at 1177. The court stated that there was still a fixation, even if there was not a complete simultaneous fixation. *Id.* at 1177-78. The court seemed to miss the point that the service provider was not challenging whether there was a fixation, but rather was arguing that the fixation did not exist for more than a transitory duration. Unfortunately, under the judge's interpretation, any service provider that processes digital communications, such as fiber optic, satellite, and some cellular communications, all of which require the conversion of the communication into a computerized form, could be held liable for infringement.

504. 17 U.S.C. § 117(2) (1994).

505. *Id.* at § 117(1).

506. *Id.* at § 101.

507. *Id.* at § 107. Fair Use is discussed in Part IX.C., *infra*.

likely, raw data is covered by an implied license which allows the work to be copied in naturally expected circumstances.

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 which includes copies in computer readable form.[508] Thus, scanned pictures, digitized sounds, machine readable texts, 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 (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, such as FTP (file transfer protocol) sites and world wide web pages. 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. The ease with which information can be accessed and duplicated has some profound copyright implications. I will use as an example a "lyric server" which is an archive that stores lyrics to songs by assorted artists.

In the case of a lyric server, 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 a potentially unauthorized copy.[509] 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 copies of his or her work.[510]

Once the file is in the archive for distribution, there may be a copyright violation every time the information is copied. While the archive user may not be making an infringing copy by just viewing the file contained in RAM,[511] if the archive is publicly accessible, viewing some types of files may possibly constitute a public performance or display[512] of the copyrighted work, the rights of which are

508. *Id.* at § 106.

509. Again this is because the Copyright Act gives the author the right to make copies and derivative works and this action constitutes making a copy.

510. 17 U.S.C. § 106(1) (1994).

511. *But see*, discussion of loading data into a computer's RAM constituting a copy, *supra* notes 501 to 506 and accompanying text.

512. Public performance and display are defined in 17 U.S.C. § 101 (1994) as:

also protected.[513] Display rights, however (as well as performance rights), are an inelegant fit in this context. When a work is transferred, it generally must be acted upon to produce a display of the work. Although some types of distribution may make the immediate display of a work a seamless process, most distribution technologies do not produce a display as a *necessary incident* of accessing the work. To infringe these display and performance rights, it should be necessary that the computer system makes the copyrighted work available in a manner such that the work is immediately shown, recited, rendered, or otherwise played directly to the user (as some types of bulletin board systems operate). To *not* require this immediate accessibility would be to confuse the right to distribute copies with the right to display or perform a work. By allowing the transmission of raw data, the system operator is making available a public place in which to *copy*, not *display*, the work. Without some activity beyond merely transmitting the work in a raw data form, to hold a system operator liable for violating a display right would be analogous to holding a place—such as a library, a newsstand, or a waiting room, or any other place which has copyrighted works available to the public—liable for violating the copyright holder's display or performance rights.

Unfortunately, courts have made just this mistake. For instance, *Playboy Enterprises, Inc. v. Frena*, involved a BBS where users could log on and download pictures scanned from the pages of Playboy magazine.[514] The BBS SYSOP claimed that he did not upload the picture files to his bulletin board system, and that it was the BBS users who both uploaded and downloaded any copies. The court held Frena liable for copyright infringement.[515] According to the court, Frena

---

(1) to perform or display it at a place open to the public or at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered; or

(2) to transmit or otherwise communicate a performance or display of the work to a place specified by clause (1) or to the public, by means of any device or process, whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same or at different times.

513. *Id.* at § 106.

514. 839 F. Supp. 1552, 1556 (M.D. Fla. 1993). *See also* Marobie-FL, Inc. v. National Ass'n of Fire Equip. Distributors and Northwest Nexus, Inc., 983 F. Supp. 1167, 1174, n.4 (N.D. Ill. 1997) (stating that a web site operator "appears to be liable" for violating the copyright holder's display right); Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc., 982 F. Supp. 503 (N.D. Ohio 1997). In another case, the plaintiff in *Playboy Enterprises, Inc. v. Sanfilippo*, No. 97-0670, 1998 U.S. Dist. LEXIS 5125 (S.D. Cal., Mar. 25, 1998) alleged that its distribution, display, and reproduction rights were infringed. The court granted an injunction allowing for all three rights; however, the court only explicitly found that the defendant had copies the plaintiff's works. *Id.* at *10-11, *20.

515. *Frena*, 839 F. Supp. at 1559.

supplied a product which the court argued contained unauthorized copies of the plaintiff's protected works, which implicated the plaintiff's exclusive right to distribute its copyrighted work.[516] Furthermore, the court held that Playboy's exclusive right to display its works was infringed.[517] Both of these holdings are arguably wrong.

When a user of Frena's BBS downloads a picture, the user is likely to see only a line indicating that the file has been transferred successfully. Viewing the picture generally requires additional steps on the part of the user.[518] It is possible that the picture will never be displayed, and will therefore never infringe the exclusive display right.

This display issue is particularly pronounced with the Web pages. With a web page, the "images" on a page will only be displayed if the user is using software that is capable of displaying images, and is using that feature.[519] Thus, which section of the Copyright Act the web page provider violates may hinge on factors not under the control of the provider.

Also at issue in the *Frena* case is the right to distribute copies.[520] The original "copy" is the one on Frena's computer's disk drive. At the end of the user transaction, this copy has not moved; it is still connected to Frena's computer. Clearly there has been no "distribution" of a copy required for an infringement of the copyright holder's distribution right. Equally clear, however, is that an infringing copy has been made. At the beginning of the transaction there was a copy only on Frena's computer. At the end of the transaction, there was also a copy on the user's computer. However, this implicates Playboy's exclusive right to make reproductions,[521] not its display or distribution rights.[522]

---

516. *Id.* at 1556. The *Sanfilippo* court cited from the same section of the *Frena* opinion in the course of its discussion of "copying." However, this part of the *Frena* opinion was specifically addressing the infringement by distribution issue. *See Sanfilippo*, 1998 U.S. Dist. LEXIS 5125, at *7.

517. *Id.*

518. Modern software packages are making the download, conversion, and display process more seamless. However, the different stages are still required, even if hidden in the background. At the time the *Frena* case was decided, the display process clearly required that multiple steps be taken by the average BBS user over which the BBS operator had no control and only presumed knowledge.

519. Not all web browsers are capable of displaying images, and most web browsers have an option to turn off the display of images in order to load web pages more rapidly.

520. 839 F. Supp. at 1556.

521. 17 U.S.C. § 106(1) (1994).

522. This same confusion over the § 106(3) distribution right was also demonstrated in the *Marobie* case. *See Marobie-FL, Inc.*, 983 F. Supp. at 1167.

The Information Infrastructure Task Force of the Commerce Department has proposed amending the copyright law to include a new "transmission right."[523] However, such a new right would do nothing but weaken the distinction between making and transmitting a copy. "Transmitting" a copy still entails the creation of new copies, which, as discussed, is already an exclusive right reserved to the copyright holder.

B. *Copyright and Strict Liability*

There is no intent or knowledge requirement to find a copyright violation. Copyright infringement is a strict liability offense—intent is only a factor in calculating damages.[524] 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.[525] Even subconscious copying has been held to be an infringement.[526] However, at least one court has limited the strict liability concept in the on-line distribution context.

In *Religious Technology Center v. Netcom On-Line Communications Service (Netcom)*, the court was squarely faced with the issue of a system operator running a machine that was passively reproducing copies of the plaintiff's work.[527] At issue was the posting of copyrighted scriptures of the Church of Scientology to a usenet news group distributed over the Internet.[528] A user posted the message to a bulletin board system, which then automatically sent the message out over a usenet news server, while archiving the message for three days. The BBS news server passed the message to the news server of Netcom,[529] the BBS' Internet provider, which then passed the message on to other news servers. In this manner, passing the message up the chain and then on to other servers worldwide, the copyrighted message rapidly reached perhaps as many as half a million news servers (which then may then make further copies for users local to each server) within a matter of a day or so. The court held that, even

---

523. *See* INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS (September 1995).

524. *Frena*, 839 F. Supp. at 1559.

525. *Id.*; *see also* De Acosta v. Brown, 146 F.2d 408 (2d Cir. 1944).

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

527. 907 F. Supp. 1361 (N.D. Cal. 1995).

528. *Id.* at 1365-66.

529. The Netcom servers archived the message for an additional eleven days. *Id.* at 1367-68.

though Netcom's servers were making copies of the Plaintiff's protected materials, the computers were making the copies without human intervention on the part of Netcom.[530] As a result, the court held it would be unreasonable to assign liability for direct copyright infringement to Netcom (or any of the other half million worldwide news server operators) where the operator could not reasonably prevent the copying, or even know that such copying was occurring, without some prior warning of what material was at issue.[531] In *Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc.*, the court held that encouraging or facilitating infringement did not amount to direct copyright infringement—some sort of volitional act on the part of the system operator is required.[532] In this case, the court found the volitional act requirement met by the service provider taking uploaded files, reviewing them, and making them available for users to download. The court rejected the argument that it was too difficult to determine which uploaded files may contain copyrighted materials that the system operator did not have the right to distribute.[533] In another more obvious case, the court in *Playboy Enterprises, Inc. v. Sanfilippo* held that a service provider could be held liable for copyright infringement for authorizing others to make infringing copies of a computer system even though the service provider had not personally made the copies.[534]

Although holding the service provider liable in such circumstances, as those present in the *Netcom* case, would be unreasonable, and although some other courts have agreed with the *Netcom* reasoning,[535] immunity from liability for the results of the passive functioning of equipment is not a necessary result under the Copyright Act. *Playboy Enterprises, Inc. v. Webbworld, Inc.* involved a web site operator which, like Netcom, made Usenet News available.[536] Unlike Netcom, however, the service provider made available a smaller subset of usenet news available—specifically pictures distributed via certain newsgroups—and added an intermediate step in the news distribution process. Specifically, the service provider had software automatically sweep the newsgroups for pictures that were posted, extract the

530. *Id.* at 1368-69.

531. *Id. See also* Sega Enterprises, Ltd. v. MAPHIA, 948 F. Supp. 923 (N.D. Cal. 1996); Sega Enterprises, Ltd. v. Sabella, 1996 WL 780560, (N.D. Cal. 1996).

532. 982 F. Supp. 503, 514-15 (N.D. Ohio 1997).

533. *Id.* at 512-13.

534. No. 97-0670, 1998 U.S. Dist. LEXIS, at *6-*9.

535. *See, e.g.*, *Marobie*, 983 F. Supp. at 1167.

536. 968 F. Supp. 1171 (N.D. Tex. 1997).

pictures, and place them on a web site for user access. Even though this process was automated, as were the reproductions in the *Netcom* case, the judge in the *Webbworld, Inc.* case held the service provider liable for infringing some of Playboy's works which were contained in some of the pictures.[537] Although the court attempted to distinguish the case in front of it from *Netcom* by arguing that Netcom is providing a different service by nature of *Netcom* also providing initial Internet access,[538] the distinction is really without relevance. In fact, the judge explicitly rejected the service provider's defense that there should be no liability as a result of the automated processes of its computers.[539]

C. *Fair Use On-Line*

Whether the unauthorized distribution or archiving of a copyrighted work 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.[540] The most important exception is the "fair use" provision.[541]

> [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 . . . .[542]

The fair use provision contains a list of uses that are presumed to be acceptable uses of copyrighted works.[543] The list includes use for criticism, comment, news reporting, teaching, scholarship, or research.[544] 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.

---

537. *Id.* at 1177.

538. *Id.* at 1175.

539. *Id.* at 1177.

540. The exceptions are codified at 17 U.S.C. §§ 107-112 (1994).

541. 17 U.S.C. § 107 (1994).

542. 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).

543. 17 U.S.C. § 107 (1994).

544. *Id.*

If a use is not one of those listed in the statute, the determination as to whether the use is "fair" is made by employing a four-factor test. The four factors are:

> (1) the purpose and character of the use, including whether such use is of commercial nature or is for nonprofit educational 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 value of the copyrighted work.[545]

Each factor is to be weighed with the others in light of the underlying purpose of awarding copyrights.[546]

Applying these factors to the System Operator's liability for a lyric server, the character of the use depends on whether access to the lyrics is available for free, or as a profit making venture and perhaps whether the archive is advertiser supported. The nature of the work is song lyrics, likely intended for commercial sale. The amount of the work used is the entire copyrighted song lyric.[547] A use of the copyrighted work which makes the original version obsolete will obviously be more likely to constitute unfair use than a use which brings more notoriety to the original.[548] 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 impact on a potential market may be substantial. For example, in a case where Playboy sued a BBS for distributing scanned images from Playboy's magazine, the BBS was found to be taking in $3 million a year, which Playboy might be able to make from its own proposed electronic service.[549]

Once again, one of the most difficult tasks for a system operator is determine which material might constitute an infringement. This is especially true since the U.S. Copyright Act no long requires placement of a copyright notice on a protected work.[550] The Copyright Act provides an author with the right to have his or her name

545. *Id.*

546. Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 578 (1994).

547. 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).

548. *Campbell*, 510 U.S. at 592.

549. *Electric Word*, WIRED, 1.1, Premiere Issue, 1993, at 24.

550. *See generally* 17 U.S.C. § 101 (1994).

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.[551]

Computer distribution often presents a whole new market for an author'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. Relying on fair use to defend archiving of works may not be 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 removed. By the time the artist protested, 240 people had already downloaded his images.[552] Such wide infringement in a potentially new market for the artist is not likely to be found by a court to constitute "fair" use.

The fair use analysis was first put to the test in *Playboy Enterprises, Inc. v. Frena.*[553] In *Frena*, a BBS made available scanned images from Playboy magazine. The System Operator claims that he did not place any of these scanned images on his system.[554] The court stated that copying can be inferred where the defendant had access to the copyrighted work, where the alleged infringing work (the scanned pictures) are substantially similar to the copyrighted work, and where one of the statutory rights guaranteed to the copyright owner is impaired by the SYSOP's actions.[555] In the case of scans made directly from a magazine publishing over 3.4 million copies each month in the United States, the first two elements of the test were easily met.[556] Frena argued that any copies of Playboy's pictures constituted fair use.[557] Employing the four fair use factors, the court held that:

1. Frena's use was clearly commercial and would likely produce future harm to Playboy's market;
2. the copyrighted works fell into the category of fiction or fantasy—entertainment rather than factual works;

---

551. 17 U.S.C. § 106A (1994).

552. Liz Horton, *Electronic Ethics of Photography; Use of Images in Desktop Publishing*, FOLIO: THE MAG. FOR MAG. MGMT., Jan. 1990, at 71. Of course, with the explosive growth of on-line services since the time of the events in this example, so too has the scope of infringement grown.

553. 839 F. Supp. 1552 (M.D. Fla. 1993).

554. *Id.* at 1554.

555. *Id.* at 1556.

556. *Id. See also*, Playboy Enterprises, Inc. v. Starware Publ'g Corp., 900 F. Supp. 433, 437 (S.D. Fla. 1995).

557. 839 F. Supp. at 1557.

3. the pictures copied from each magazine constituted an essential part of the copyrighted work (the magazine); and
4. the effect of copying the Plaintiff's work would be detrimental to the potential market of the copyrighted work.[558]

D. *Contributory and Vicarious Infringement*

The language of the Copyright Act does not limit its scope of application to direct infringements.[559] There are two types of third party liability that may be present: one is contributory liability (summarized as "knowledge and participation" in the infringing activity),[560] and the other is vicarious liability (summarized as "benefit and control" of the infringing activity.[561] These two types of liability are often hard to distinguish from one another.

The proper circumstances for finding contributory infringement are those in which the third party has knowledge of and participates in the direct infringement of a protected work.[562] The oft-cited definition of a contributory infringer is "[o]ne who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another."[563] Thus, contributory infringement requires a "know or has reason to know" standard.[564] Even constructive knowledge may be adequate, at least where potentially infringing activities are encouraged by the service provider who stands to benefit

---

558. *Id.* at 1558-59.

559. *See* Banff Ltd. v. Limited, Inc., 869 F. Supp. 1103, 1107 (S.D.N.Y. 1994), where the court noted:

> 17 U.S.C. § 501(a) (1994) declares that "[a]nyone who violates any of the exclusive rights of the copyright owner . . . is an infringer of the copyright." The language of the statute thus raises the question of when such rights have been 'violated,' a formulation that by its terms does not limit liability to direct actors.

560. Religious Technology Center v. Netcom On-line Communication Services, Inc. 907 F. Supp. 1361, 1375 (1995).

561. *Religious Technology Center*, 907 F. Supp. at 1375, *citing* Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 306 (2d Cir. 1963).

562. Singer v. Citibank, N.A., No. 91 Civ. 4453, 1993 WL 177801 (S.D.N.Y. May 21, 1993).

563. See also Casella v. Morris, 820 F.2d 362, 365 (11th Cir. 1987); Columbia Pictures Industries, Inc. v. Redd Horne Inc., 749 F.2d 154, 160 (3d Cir. 1984); Gershwin Publ'g Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir. 1971); Polygram Int'l Publ'g, Inc. v. Nevada/TIG, Inc., 855 F. Supp. 1314, 1333 (D. Mass. 1994); F.E.L. Publications, Ltd. v. National Conference of Catholic Bishops, 466 F. Supp. 1034, 1040 (N.D. Ill. 1978).

564. *See, e.g.*, *Casella*, 820 F.2d at 365-66. In *Casella*, a business owner who sold a restaurant, complete with singing robots, was considered a contributory infringer when he did not inform the business purchaser that the license to the songs sung by the robots had been revoked. He knew the new owners would wind up infringing, and did not inform them that their expected actions were in violation. Therefore, his sale "induced" these violations. *Id.*

from the presence of potentially infringing files on its system.[565] This test also requires that the function of the contributor be looked at in the infringing process, and not just the "quantitative contribution" of the infringer.[566] If the person authorizes the use of a work without the permission of the copyright holder, and was in a position to control the use of the copyrighted works by others, then that person can be held liable as a contributory infringer.[567]

Sega v. MAPHIA held that a SYSOP can be liable for copyright infringement where he played a part in the distribution of copyrighted software via his BBS.[568] At issue in *Sega* was a members-only bulletin board system used to distribute copyrighted video games.[569] Access was given either in exchange for money, for supplying copyrighted games, or to the defendant's customers who had bought devices used to read the software from the original game cartridges.[570] The court held that the defendant knew about and encouraged the use of his system for the copying of Sega's copyrighted works.[571] Furthermore, the court held that unauthorized copies of the videogames were made every time a game was uploaded to or downloaded from the bulletin board,[572] and that once downloaded, other copies were then made by the BBS users.[573] This additional copying was facilitated and encouraged by the BBS administration. Thus, the court dismissed the defendant's fair use argument by pointing out how each of the fair use factors weighed against the defendant's use being a fair one.[574]

Another case that addressed the issue of contributory infringement was the *Netcom* case discussed above. In *Netcom*, the court held that a finding of contributory infringement was possible if it could be

---

565. Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc., 982 F. Supp. 503, 514-15 (N.D. Ohio 1997).

566. *Gershwin*, 443 F.2d at 1162, *quoting* Fortnightly Corp. v. United Artists Tele. Inc., 392 U.S. 390, 396-97 (1968).

567. Cable/Home Communication Corp. v. Network Prods. Inc., 902 F.2d 829, 845 (11th Cir. 1990).

568. Sega Enterprises v. MAPHIA, 948 F. Supp. 923, 933 (N.D. Cal. 1996).

569. *Id.* at 927-28.

570. *Id.* at 928-29. One of the defendants sold "copiers" which are devices used to read the software from a game cartridge for saving to a floppy disk, or for playing software from a disk on one of Sega's game consoles.

571. *Id.* at 932.

572. *Id.*

573. *Id.* at 932-33.

574. *Id.* at 936. In an earlier decision, *Sega Enterprises v. MAPHIA*, 857 F. Supp. 679, 687 (N.D. Cal. 1994), the court found that in order to employ the fair use exception, one must possess a legal copy in the first place.

shown at trial that the service provider knew that its service was being used to infringe the plaintiff's copyrights, and yet the defendant did not take what steps it could to prevent or otherwise mitigate the damage caused by the infringement.[575] The court held that an Internet service provider is more than a landlord who merely provides facilities.[576] Rather, the provider is more akin to the radio stations that have historically been found liable for rebroadcasting an infringing broadcast.[577]

The second type of third-party liability is vicarious liability. Vicarious liability attaches when, even in the absence of knowledge of the infringement, a party has the "right and ability" to supervise the infringing activity of another, and derives "obvious and direct financial interest in the exploitation of copyright materials."[578] Vicarious liability cases are often analyzed based on two lines of cases: landlord-tenant cases, which exempt from liability landlords who receive only a fixed rent and receive no additional financial benefit from any infringement;[579] and "dance hall" cases, where nightclub owners have been held vicariously liable for infringing music played by bands performing in the clubs.[580] Courts faced with vicarious liability cases have had to place the infringing activity somewhere on this spectrum.[581]

The theory behind vicarious liability is that:

> The law of vicarious liability treats the expected losses as simply another cost of doing business. The enterprise and the person profiting from it are better able than either the innocent injured plaintiff or the person whose act caused the loss to distribute the costs and to shift them to others who have profited from the enterprise. In addition, placing responsibility for the loss on the enterprise has the added benefit of creating a greater incentive for

---

575. *Religious Technology Center*, 907 F. Supp. at 1374-75.

576. A landlord is not liable for infringements occurring on the premises. *See, e.g.*, Deutsch v. Arnold, 98 F.2d 686, 688 (2d Cir. 1938).

577. *Religious Technology Center*, 907 F. Supp. at 1375; *see also* Select Theatres Corp. v. Ronzoni Macaroni Corp., 59 U.S.P.Q. 288, 291 (S.D.N.Y. 1943).

578. Shapiro Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 307 (2d Cir. 1963). *See* KECA Music, Inc. v. Dingus McGee's Co., 432 F. Supp. 72, 74-75 (W.D. Mo. 1977); *Gershwin*, 443 F.2d at 1162. *See also* Unicity Music, Inc. v. Omni Communs., Inc., 844 F. Supp. 504, 509 (E.D. Ark. 1994) (radio station manager who also owned the corporation was liable for the station's infringement); Boz Scaggs Music v. KND Corp., 491 F. Supp. 908, 913 (D. Conn. 1980) (manager of radio station liable for station's infringements); Artists Music, Inc. v. Reed Publishing, Inc., 31 U.S.P.Q.2d 1623, (S.D.N.Y. 1994); *Singer*, 1993 WL 177801, at *1.

579. *See, e.g.*, *Deutsch* 98 F.2d at 686.

580. *See, e.g.*, *Shapiro*, 316 F.2d at 307; *Polygram*, 855 F. Supp. at 1324.

581. *Polygram*, 855 F. Supp. at 1324.

> the enterprise to police its operations carefully to avoid unnecessary losses.[582]

This is true even where the vicarious infringer does not have actual knowledge of the infringement. The claim is that the vicarious infringer should either pay more attention, or should bear the loss instead of the copyright owner.[583]

Even a passive actor who derived benefit from the infringement can be held "responsible for the policy of neglect which resulted in the infringement of the Plaintiff's copyright interests."[584] Even if the infringing acts were performed by an independent contractor, there is still vicarious liability for the party who had the right and ability to supervise the infringer's activities,[585] under the theory that the supervisor should not profit from the infringing behavior of another whom the supervisor could have controlled.[586] Furthermore, a corporate officer who either has direct participation or financial interest in the infringement may be directly liable for the corporation's infringement.[587]

The *Netcom* court also addressed the vicarious liability issue. In that case, the court found the plaintiff's claim of vicarious infringement meritless.[588] While there was evidence to suggest that Netcom had the right and ability to supervise the acts of the infringer by nature of Netcom's service agreement, indemnity agreement, and its ability to keyword-screen messages passing through its system, the financial benefit prong was not met. Because Netcom received a fixed-fee from its subscribers, it received no additional financial benefit from the infringement, and, thus, there was no vicarious infringement.[589]

---

582. *Id.* at 1325.

583. *Id.*

584. Sailor Music v. IML Corp., 867 F. Supp. 565, 569 (E.D. Mich. 1994).

585. *Fourth Floor*, 572 F. Supp. at 43.

586. *Artists Music, Inc.* 31 U.S.P.Q.2d at 1626.

587. Playboy Enterprises, Inc. v. Starware Publishing Corp., 900 F. Supp. 438 (S.D. Fla. 1995). *See also* Playboy Enterprises, Inc. v. Webbworld, Inc., 968 F. Supp. 1171 (N.D. Tx. 1997).

588. *Religious Technology Center*, 907 F. Supp. at 1377.

589. *Id. See also, Marobie*, 983 F. Supp. at 1177. *But see Webbworld, Inc.*, where the defendants were held vicariously liable for running a fixed-fee pay usenet news service where some of the posts available via the service infringed the plaintiff's copyrights. 968 F. Supp. at 1173. It is worth pointing out that this author does not place great weight on the financial benefit prong of the vicarious infringement test. While there is a long line of cases that state that this requirement must be met, the requirement appears to be based on an old version of the Copyright Act. In subsequent revisions to the Copyright Act, the provision requiring financial benefit has been explicitly removed, yet the cases all cite back to earlier cases from before the law change. Additionally, this financial benefit prong raises questions as to whether a service provider will risk

E. Liability for Web Links

To examine how the copyright liability applies to a web provider,[590] we must first examine how the Web works.

To call up a document on the Web, a user connects to the Web provider's web server. There, the user is presented with a "homepage," which is the introductory hypertext document. By selecting the various hypertext links, "copies" of other documents[591] (or subpages) are "transmitted" to the user. These documents may be transmitted directly to the user by the Web provider, if the documents reside on the initially-contacted web provider's computer. However, it is often the case that these documents reside on a web page on another computer somewhere else on the computer network (referred to here as the "secondary computer"). These secondary computers are potentially anywhere in the world. Thus, the hypertext link serves as an address, much like a listing in a bibliography, or, more accurately, like a description of a place on the shelf in someone else's library where the book is stored.

The user's "web browser" software reads this listing (the hypertext link), and then uses it to request a copy of the document from the secondary computer that stores the document at the location indicated by the hypertext link. If the document is not stored on the initial web provider's computer, then the initial web provider provides the address of the linked item on the secondary computer. It is the user who then transmits a request to the secondary computer, as recommended by the initial computer, which results in the secondary computer transmitting a copy of the requested file. If the secondary computer is not available, or if the remote file is password-protected or otherwise limited in its access, then the work will not be transmitted at the user's request, and the user will receive only an error message or will be prompted for a password. It is as if the bibliography refers the user to a book that is missing from the shelf of the distant library, or is in a library for which the user does not have a library card.

---

greater liability by providing "metered service"—where the cost of users' service is based on the volume of network bandwidth used by that customer.

590. To avoid additional levels of complexity, the discussion of web providers assumes that the entity that designs and maintains the web page is also providing the web page on the entity's own "web server," as opposed to having the web page actually made available by some third party, such as on a university or commercial service provider's computer. A website saver is a computer which runs web software and "serves up" the requested files.

591. Which could be text, pictures, motion pictures, sounds, or software files.

The initial web provider has no control over what is provided at the secondary site, but the initial provider must program the link to the secondary site if it is to be accessible from the initial web page in the first place. In other words, the book may be in the library, but the Web user would either not know that it exists, or would not be able to get it as a result of the information provided by the initial web page. It is also possible that, after the link is made, another "book" could be put in the same "place on the shelf." In essence, a web page provider could link to Document A at a distant site, and at some point later, the distant site could replace Document A with Document B. The only way for the initial web provider to know of the switch in documents would be to follow the link and see that Document B has been substituted in place of Document A, the document originally linked on the homepage.

Another way of examining the situation is as follows: accessing a link which calls up a document distributed from a web server to which you are directly connected is the equivalent to sending a request to that web page's computer saying, "transmit to me the file stored on your machine at the location specified in this link." At this point, if the user has the appropriate permission,[592] the indicated work is sent. If the file is not stored on the machine running the web page the user is accessing, then accessing a link is the equivalent to saying to the initial web provider's computer, "you are indicating to me that I can access a copy of Document A at this distant location, and I would like to access Document A." At this point, a request for a transmission of the document stored at the link's destination is sent by the user to the secondary computer recommended by the initial computer. If the user has the appropriate permission, a "copy" of the document is then "sent" to the user's computer.

If the document accessed on the web page is stored locally, then the copyright analysis is fairly straight forward. The document is read from the web provider's disk drive and into the RAM of the web provider's computer, creating a copy.[593] The work is then transmitted through the computer network and "fixed" in the RAM of the user's computer. The work has now been reproduced, implicating

592. In other words, if the document is "world readable" or if the user has any passwords necessary to access the document, the user has appropriate permission.

593. MAI System Corp. v. Peak Computer, Inc., 991 F.2d 511, 519 (9th Cir. 1993); Advanced Computer Services of Michigan, Inc. v. MAI Systems Corp., 845 F. Supp. 356, 363 (E.D. Va. 1994); Triad Systems Corp. v. Southeastern Express Co., 31 U.S.P.Q.2d 1239, 1242 (N.D. Ca. 1994), *cert. denied*, 516 U.S. 1145 (1996).

rights[594] of the copyright holder (who, of course, may be the web provider). Any of these copies may be infringing copies.[595] In many cases the work will be put up on the web page by or under the authority of the copyright holder, in which case the copies would be ones that are either explicitly permitted, or presumably subject to an implied license by nature of their being made available on a web page that requires such reproductions to be made in order to view the work.[596]

If the document accessed is not located on the web provider's computer, and is "linked" only on the provider's web page while residing on another computer, the situation becomes a bit more complicated. In this situation, the web provider is not delivering the document directly, and no copy ever comes into contact with the initially-accessed web provider's computer. The initial web provider does not transmit anything to the user other than the location of the work on the secondary provider's computer. Because of this, there can be no direct liability if the transferral of the work constitutes an infringement. It then becomes necessary to determine whether the initial provider is either contributorily or vicariously liable for the infringement.

As stated earlier, "one who, with knowledge of the infringing activity, induces, causes, or materially contributes to the infringing conduct of another, may be held liable as a 'contributory' infringer."[597] In order for a web operator to be liable to an "infringing site" for placing a link on its web page,[598] the web operator does not have to actually know or have reason to know of the infringements that are likely to occur as a result of the user accessing the infringing site.[599] Actual knowledge that the link will result in infringements is not required; reason to know on the part of the web operator will suffice.[600] Moreover, it is not important that the user is doing the

594. 17 U.S.C. § 106(1) (1994).

595. A&M Records, Inc. v. An Internet Site Known as Fresh Kutz, No. 97 CV 1099H (JFS) (S.D. Cal. June 10, 1997).

596. *C.f.*, Effects Associates, Inc. v. Cohen, 908 F.2d 555 (9th Cir. 1990); Oddo v. Ries, 743 F.2d 630 (9th Cir. 1984).

597. *Gershwin*, 443 F.2d at 1162.

598. For these purposes, an "infringing site" is defined as a web page which will transmit copyrighted material when accessed as a result of a user following the link provided on the initial web page, or a page which is linked for the purpose of accessing infringing material contained thereon, even if the infringing material is not immediately transmitted as a result of the initial link.

599. *See, e.g.*, *Casella*, 820 F.2d at 364-65.

600. *Cf.* Cable/Home Communication Corp. v. Network Productions, Inc., 902 F.2d 829, 846 (holding defendants violated copyright law by creating and distributing pirate computer chips

actual infringing, as long as the user is doing the infringing through the initial web provider's web page.[601] Even though all that is being provided by the initial web page is a form of advertising for the infringing site, in other contexts, cases have held that contributory liability could be found if an advertiser knew that the product being promoted was an infringing one.[602] In such a case, not only is the infringing site being "advertised" by the initial site, but the initial site is also giving the user a head start on any infringement. While the user may be able to gain knowledge of the infringing site without the help of the initial page, the assistance provided by the initial site is possibly material enough to constitute contributory infringement.

When there is no contributory liability, the web provider may still be vicariously liable for linking to an infringing site. This would apply to situations where a link is put on the initial page to a secondary site that is making infringing works available, unbeknownst to the initial page provider. In some ways, if a web operator links to a site containing copyright violations, the situation is analogous to the bars in the "dance hall cases" who invite in "guests" (web page users) to enjoy the "performances" (links) that the proprietor is making available, even if the performers (sites linked) are "independent contractors."[603] In other words, the web page provider is more like a landlord. The web provider provides the link, but is not in a position to supervise or control the conduct of the infringing site.[604] The most control that the web provider (the "landlord") could have over the secondary provider (the "tenant"), is by removing the link from the initial web page (in essence, by "eviction").

Case law in the vicarious liability area is unclear and inconsistent. The majority of the parent/subsidiary vicarious infringement cases have held that a parent corporation is not liable for the infringing activities of its subsidiary, unless some actual involvement can be

---

which enabled display of programs intended for paying subscribers). See also Singer v. Citibank, N.A., No. 91 Civ. 4453, 1993 WL 177801 (S.D.N.Y. May 21, 1993).

601. *Cf.* M. Whitmark & Sons v. Tremont Social & Athletic Club, 188 F. Supp. 787, 789 (D. Mass. 1960) (holding performance of copyrighted music by orchestra which played on weekends was a "public playing for profit" and rendered the club liable for infringement). *See also* Dreamland Ball Room, Inc. v. Shapiro, Bernstein & Co., 36 F.2d 354, 355 (7th Cir. 1929).

602. *See* Columbia Pictures Indus. Inc. v. Redd Horne, Inc., 749 F.2d 154, 160; Screen Gems-Columbia Music, Inc. v. Mark-fi Records, Inc., 256 F. Supp. 399, 404-05 (S.D.N.Y. 1966).

603. *See, e.g.*, Famous Music Corp. v. Bay State Harness Horse Racing and Breeding Ass'n, Inc., 554 F.2d 1213, 1214 (1st Cir. 1977); *Dreamland Ball Room*, 36 F.2d at 355; KECA Music, Inc. v. Dingus McGee's Co., 432 F. Supp. 72, 74-5 (W.D. Mo. 1977).

604. *Cf.*, Deutch v. Arnold, 98 F.2d 686, 687-88 (2d Cir. 1938) (holding that a handwriting analysis chart made by a person having access to the copyrighted handwriting chart infringed on the copyrighted chart).

shown,[605] though a minority have been more willing to make the stretch necessary to find liability.[606]

In the end, vicarious liability poses a tough question, and the likelihood of finding an infringement will hinge on whether the merits of the case warrant such a finding, and then only if direct or contributory liability cannot be found.

F. *Copyright Infringement as Wire Fraud*

In addition to using traditional theories of copyright infringement to challenge infringers, some prosecutors have tried employing some creative alternatives. A controversial case worth mentioning is one in which prosecutors tried to convict a BBS operator of conspiring to commit wire fraud. In *United States v. LaMacchia*, the court held though that the wire fraud statute could not be applied to LaMacchia's conduct, due to the fact that his bulletin board system was used to distribute copyrighted software without charge.[607] The *LaMacchia* court based its decision on the precedent set by the U.S. Supreme Court case *Dowling v. United States*.[608]

At issue in *Dowling* was the transport through the mail of bootleg Elvis records. The government had accused Dowling of violating the mail fraud statute, after which the wire fraud statute is modeled. The government claimed that the bootleg records constituted property "stolen, converted, or taken by fraud" as covered by the Interstate Transportation of Stolen Property Act. In his opinion, Justice Blackmun reasoned that copyrighted works were not tangible property of the sort normally covered by the Stolen Property Act.[609] Because no transfer of the copyright had taken place, there had been no theft of the copyright, only an infringement of it.[610] However, such infringements are addressed by the Copyright Act.[611] Therefore, the government was incorrect in trying to apply a "gap filler" statute, such as the Stolen Property Act, to cover the interstate sale of record albums

605. *See* Banff Ltd. v. Limited, Inc., 869 F. Supp. 1103, 1108 (S.D.N.Y. 1994). *See also* Howard Johnson Co., Inc. v. Khimani, 892 F.2d 1512, 1518 (11th Cir. 1990); Frank Music Corp. v. Metro-Goldwyn-Mayer Inc., 886 F.2d 1545 (9th Cir. 1989); Artists Music, Inc. v. Reed Publishing, Inc., 31 U.S.P.Q.2d 1623 (S.D.N.Y. 1994).

606. *See, e.g.*, Broadcast Music, Inc. v. Hartmarx Corp., No. 88C 2856, 1989 WL 121290 (N.D. Ill. Oct. 5, 1989).

607. 871 F. Supp. 535, 545 (D. Mass. 1994).

608. 473 U.S. 207 (1985).

609. *Dowling*, 473 U.S. at 228.

610. *Id.* at 218-19.

611. *Id.*

that, while not stolen, contained unlawful recordings.[612] Rather, the Stolen Property Act was meant to protect the owner of an item from being deprived of that item's possession; not as a result of the creation and sale of the Elvis records.[613]

Justice Blackmun pointed out that the Copyright Act applies the term of art "infringement" for such actions, instead of using the more common terms "theft", "conversion", or "fraud."[614] Justice Blackmun reasoned that, because the Copyright Act clearly applied to Dowling's conduct and provided appropriate penalties for that conduct, it would be inappropriate to stretch another statute to cover actions clearly under the disposition of the Copyright Act, merely because interstate transportation was involved.[615] However, the recordings that were transported, while not amounting to theft, were subject to mandatory licensing fees, which Dowling did not pay.[616]

In the *LaMacchia* case, unlike in *Dowling*, no underlying fraud was found.[617] This was because the computer software in *LaMacchia*, unlike in *Dowling*, was protected by the copyright law but was not subject to a licensing fee.[618] There was no concealment of unpaid royalties, nor wire fraud. The felony copyright infringement statute could not be applied to LaMacchia to find criminal infringement, because the statute requires that the defendant must have infringed the copyright "willfully and for purpose of commercial advantage or private financial gain."[619] While LaMacchia was willful in setting up and running his pirate bulletin boards, he did not intend to profit by his actions. Thus, while he may have been a software pirate, he was not a criminally-infringing one.[620]

In cases such as *LaMacchia*, the copyright Act does provide a remedy for aggrieved copyright holders. Therefore, creative attempts at prosecution such as attempted in *LaMacchia*, and reactionary legislative regulation, such as the "No Electronic Theft Act," passed to close the "*LaMacchia* loophole," are unnecessary and risk causing

612. *Id.* at 226-27.
613. *Id.* at 228.
614. *Id.* at 217.
615. *Id.* at 218.
616. *Id.*
617. *La Macchia*, 871 F. Supp. at 542-43.
618. *Id.*
619. 18 U.S.C. § 2319 (1994).
620. Since this case was decided, the "No Electronic Theft Act" (Pub. L. No. 105-147, 111 Stat. 2678, Dec. 16, 1997) (not currently codified) was signed into law to specifically address the holding of this case and to extend the criminal copyright infringement penalties to cover certain acts of not-for-profit copying.

more harm than good to the balance of rights established by the Copyright Act.

X. TRADEMARK & UNFAIR COMPETITION ISSUES

A. *Confusion*

Along with copyright issues, trademark and unfair competition issues are growing concerns in the on-line world. Two of the copyright cases mentioned earlier held that distribution of copyrighted material amounted to violation of the copyright holder's trademark, as well as unfair competition.[621]

Federal trademark law provides that:

> (a) Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which—
>
> (1) is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person, or
>
> (2) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities, shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.[622]

Section 1125 serves to prevent an infringer from using another's trademark in competition with the rightful trademark holder.[623] It prohibits attempts or actions likely to result in an infringer's "passing off" its products or services for the products of another.[624] Merely using another's trademark on-line does not necessarily constitute trademark infringement.[625]

The *MAPHIA* court applied section 1125 in the copyrighted software context, and found that the distribution of copyrighted video

621. Sega Enterprises v. MAPHIA, 857 F. Supp. 679, 688-89 (N.D. Cal. 1994); Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552, 1560, 1562 (M.D. Fla. 1993).

622. 15 U.S.C. § 1125 (1998). This is also known as Section 43 of the Lanham Act.

623. *See, e.g.*, 20th Century Wear, Inc. v. Sanmark-Stardust, Inc., 747 F.2d 81 (2d Cir. 1984), *cert. denied*, 410 U.S. 1052 (1985).

624. *See, e.g.*, Dorr-Oliver, Inc. v. Fluid-Quip, Inc., 94 F.3d 376 (7th Cir. 1996).

625. Patmont Motor Werks, Inc. v. Gateway Marine, Inc., No. C 96-2703 1997 WL 811770 (N.D. Cal. Dec. 18, 1997).

game software amounted not only to a violation of Sega Enterprise's (Sega) copyright, but such distribution was also a violation of Sega's trademark rights and amounted to unfair competition under the federal trademark law.[626] The court stated that every time a game was downloaded and subsequently played, Sega's trademarks were used.[627] Sega's trademarks were also used in the file descriptors of the games stored on the BBS.[628] Downloaded games enter the stream of commerce, potentially causing confusion as to their origin. This practice deprived Sega of revenue, made available confidential prerelease versions of some of its games, and made games available without proper packaging and instructions.[629] All of these practices potentially caused damage to Sega's business and reputation in violation of the Trademark Act. Thus, knowing distribution of trademarked software resulted in liability for the BBS operators.[630]

Similarly, the BBS operator in the *Frena* case was held liable for trademark infringement and unfair competition because he distributed trademarked pictures on his bulletin board system.[631] As the *MAPHIA* court held in the software context, the *Frena* court held that the System Operator's use of the Plaintiff's trademarked works violated Playboy's trademark rights and constituted unfair competition.[632]

While both of these cases involved U.S. plaintiffs and U.S. defendants, it would be a further violation of the Lanham Act to import infringing goods into the United States.[633] Accessing a non-U.S. computer information service, by modem or computer network, which contains trademarked materials, and then downloading these materials into the United States may constitute an importation, as the statute is not limited to specific modes of transporting the imported materials.

However, it is possible that computer information system operators may be given a small measure of protection under the Lanham Act for unknowingly transmitting trademark infringements

626. 857 F. Supp. at 688-89.

627. *Id.* at 684.

628. *Id.*

629. *Id.*

630. *Id.*

631. *See Frena*, 839 F. Supp. at 1560-1562.

632. *Id.* at 1561-62.

633. The Statute reads, in part:

> (b) Any goods marked or labeled in contravention of the provisions of this section shall not be imported into the United States or admitted to entry at any customhouse of the United States . . .

15 U.S.C. § 1125(b).

effectuated by the system's users if the SYSOPs are deemed to be "innocent infringers" who are "engaged solely in the business of printing the mark or violating matter for others."[634]

B. Dilution

Trademark dilution in the computer-communication context is becoming an increasingly important issue. Nearly half of the U.S. states have a trademark "dilution" or "anti-dilution" statute that protects trademarks even where there is no likelihood of confusion between two uses of a mark.[635] Because this produced patchwork protection of what is often a national concern, the Federal Dilution Act was passed, which adds subsection (c) to Section 43 of the Lanham Act[636] to provide protection against dilution for "famous" marks.[637] The Act provides:

> The owner of a famous mark shall be entitled, subject to the principles of equity and upon such terms as the court deems reasonable, to an injunction against another person's commercial use in commere of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark.[638]

The Dilution Act also explicitly allows for "fair use" of a famous mark for purposes such as news reporting, parody and certain other sorts of noncommercial uses.[639]

---

634. 15 U.S.C. § 1114 (2) (1986).

635. Summary of Testimony of the International Trademark Association on H.R. 1295 and 1270 *available in* 1995 WL 435750 (July 19, 1995).

636. Federal Trademark Dilution Act of 1995, 104th Cong., 1st Sess., 141 Cong. Rec. H14317 (1995) (codified at 15 U.S.C. § 1125(c) (West Supp. 1996)).

637. To be considered a famous mark, section 1125 (c) provides that courts are to consider the following list of factors:

> (A) the degree of inherent or acquired distinctiveness of the mark;
> (B) the duration and extent of use of the mark in connection with the goods or services with which the mark is used;
> (C) the duration and extent of advertising and publicity of the mark;
> (D) the geographical extent of the trading area in which the mark is used;
> (E) the channels of trade for the goods or services with which the mark is used;
> (F) the degree of recognition of the mark in the trading areas and channels of trade used by the marks' owner and the person against whom the injunction is sought;
> (G) the nature and extent of use of the same or similar marks by third parties; and
> (H) whether the mark was registered . . .

638. 15 U.S.C.A. § 1125(c)(1).

639. 15 U.S.C. § 1125(c). *See also* Summary of Testimony of the International Trademark Association on H.R. 1295 and 1270, *supra* note 635. Failure to consider these free speech implications caused an earlier attempt to pass such a dilution statute to fail. *See* David S. Villwock, *The Federal Dilution Act of 1995*, 6 DEPAUL-LCA J. ART & ENT. L. 213, 221 (1996).

Traditionally, trademark dilution comes in one of two forms: tarnishment or blurring. Dilution by tarnishment occurs when a famous mark is linked to poor quality or unwholesome products, or otherwise displayed in a derogatory manner.[640] If the use of the mark does not result in negative associations for the senior trademark user, then there is no dilution by tarnishment.[641]

Dilution by blurring involves a "whittling away" of the value and selling power of a mark by its unauthorized use.[642] The Dilution Act is intended to prevent only cases where actual blurring may occur.[643] For instance, blurring occurs where one uses another's mark in the same specialized industry, or when both uses occur on products intended for the general public, but not necessarily where a use is in a specialized industry and the other use is in another, unrelated specialized industry.[644]

Unlike traditional trademark infringement, it is not necessary that the goods or services compete, or that there is a likelihood of confusion between the competing uses of a mark. To find blurring under the Dilution Act, one court has identified five relevant factors: "1) similarity of the trademarks and trade dress; 2) similarity of the products; 3) sophistication of consumers; 4) renown of the senior mark and trade dress; and 5) renown of the junior mark and trade dress."[645] While the first three factors are similar to the likelihood of confusion test, what is important to remember is that any use which increases the possibility of a mark losing its distinctiveness may constitute dilution by blurring.[646]

C. *The Law Applied*

The majority of the trademark cases involving computer networks have been Internet domain name cases. A domain name is a form of address[647] that indicates the location of a computer connected to the

---

640. Panavision Int'l, L.P. v. Toeppen, 945 F. Supp. 1296, 1304 (C.D. Cal. 1996).

641. *See, e.g.*, Clinique Lab., Inc. v. Dep Corp., 945 F. Supp. 547, 562 (S.D.N.Y. 1996).

642. *Panavision Int'l, L.P.*, 945 F. Supp. at 1304.

643. Summary of Testimony of the International Trademark Association on H.R. 1295 and 1270, *supra* note 635. *See also* Megan E. Gray, *Defending Against a Dilution Claim: A Practitioner's Guide*, 4 TEX. INTELL. PROP L.J. 205, 210-11 (1996).

644. *Id.*

645. *Clinique Lab., Inc.*, 945 F. Supp. at 562. *See also* Merriam-Webster, Inc. v. Random House, Inc. 35 F.3d 65, 73 (2d Cir. 1994).

646. *Id.* (citing Deere & Co. v. MTD Prods., Inc., 41 F.3d 39, 43 (2d Cir. 1994)).

647. The basic Internet address is in numerical form (the "IP" address, or "Internet Protocol" address). The domain name address is an alphanumeric address which exists to make Internet addresses easier to remember. *See, e.g.*, MTV Networks v. Curry, 867 F. Supp. 202,

Internet and the type of organization or the country to which the address belongs.[648]

These addresses are valuable assets to companies seeking to establish a corporate presence on the Internet because of the network's commercial potential.[649] As companies and individuals become increasingly aware of the value of these addresses, which are assigned primarily on a first-come/first-served basis,[650] companies have either had to fight to regain domain names that match the names of their companies and have been registered by others, or fight to prevent the use of domain names that are likely to confuse consumers into believing that the services offered at that location on the Internet are associated with their company when the services are really being provided by another entity.[651]

A clear example of the confusion over domain names is the conflict between competing test preparation companies Princeton Review and Stanley Kaplan Review. The Princeton review registered the domain names "princeton.com" and "review.com," but they also registered "kaplan.com" in order to "mock and annoy" its competitor.[652] The Princeton Review used the site to provide people, who were looking for Kaplan Review's materials, with electronic materials critical of the quality of Kaplan's services and explaining why they believed the Princeton Review was better. Kaplan sued to recover "its" address (after refusing the Princeton Review's offer to turn over the address in exchange for a case of beer). The case was resolved, after it was removed to binding arbitration, in favor Kaplan.[653]

Another early conflict over domain names included author Joshua Quittner's registration of the domain name "mcdonalds.com" in the course of writing an article on businesses that fail to register their corporate names as Internet sites.[654] The first conflict to produce a

---

204 (S.D.N.Y. 1994) (involving summary judgment motions on fraud and breach of contract claims, and did not address the trademark issues or the merits of the unfair competition claim).

648. Dan L. Burk, *Trademarks Along the Infobahn: A First Look at the Emerging Law of Cybermarks*, 1 RICH. J.L. & TECH. ¶ 24 (Apr. 10, 1995).

649. *Curry*, 867 F. Supp. at 207.

650. *Id.* at 204.

651. For a good account of many of these conflicts see *Burk*, *supra* note 648.

652. *Id.* at paragraph 19.

653. *Id.* Apparently no beer was exchanged in settlement and the president of Princeton review accused his rival of having "no sense of humor, no vision, and no beer" and he vowed to register the domain name "kraplan.com" in order to distribute electronic materials disparaging of his competitor. *Id.* at paragraph 20.

654. *Id.* at paragraph 21. This conflict was settled in exchange for McDonald's donating $3,500 worth of computer equipment to a grade school for connecting the school to the Internet. *Id.* at paragraph 21.

court decision involved Adam Curry's use of the domain "mtv.com," and MTV's attempt to acquire that address.[655] The case settled out of court, and MTV now owns the "mtv.com" domain, while Curry has moved his information system to the "metaverse.com" address.[656]

Taking advantage of the Dilution Act, Hasbro became the first company to enjoin the use of an Internet domain name. In *Hasbro, Inc. v. Internet Entertainment Group Ltd.*, the use of the address "candyland.com" by an adult-entertainment provider was enjoined because it diluted Hasbro's trademark.[657] This case also presented a good example of tarnishment because the mark for a children's board game was used to label an adult entertainment site.

Shortly after the *Hasbro, Inc.* case was decided, the case of *Comp Examiner Agency, Inc. v. Juris, Inc.* produced an injunction based on a likelihood of confusion over the use of a domain name.[658] This case involved the defendant using a web page to advertise products aimed at the same target market as that of the plaintiff's products. The court held that the plaintiff was likely to succeed in showing that there was a likelihood of confusion between the two uses of the "juris" mark, and therefore the defendant was enjoined from using the "juris.com" domain name.[659]

Another more straightforward case was *Digital Equipment Corp. v. Altavista Technology, Inc.*[660] The case involved a preliminary injunction granted following a dispute over the use of the name "AltaVista" on the Internet. When the Plaintiff created the "Alta-Vista" search engine, it bought the trademark rights to use the name from AltaVista Technology, Inc. (ATI) and licensed back to ATI certain rights in the name.[661] One of the rights ATI retained was the right to use the <http://www.altavista.com/> web page address. As Digital's search engine, located under the Digital domain name at <http://www.altavista.digital.com/>, became more popular, large numbers of people accidentally looked for the engine at ATI's web address, a natural error to make. ATI placed a link on its web page

---

655. *Curry*, 867 F. Supp. at 207. Curry was formerly employed at MTV as a "VJ" (Video Jockey), and was an MTV employee when he established the domain name.

656. *See Burk*, *supra* note 648 at paragraph 17.

657. No. C 96-130, 1996 WL 84858 (W.D. Wash. Feb. 22, 1996).

658. Comp Examiner Agency, Inc. v. Juris, Inc., No. 96-0213 1996 WL 376600 (C.D. Cal. Apr. 26, 1996).

659. *Id.* Another similar case involved use of the domain name "cardservice.com" to promote credit and debit card processing services. Cardservice International, Inc. v. WRM & Assoc., 950 F. Supp. 737 (E.D. Va. 1997).

660. 960 F. Supp. 456 (D. Mass. 1997).

661. *Id.* at 458.

to the real address of Digital's search engine. As the traffic increased, however, ATI redesigned its web page to look more and more like that of the Digital search engine, and then began selling advertising to companies that thought they were buying ad space at the search engine site. The court found that ATI had exceeded its rights under the license agreement with Digital, and that its actions constituted unfair competition and an infringement of Digital's trademark rights in violation of 15 U.S.C. § 1125(a).[662] When looking at the factors leading to a likelihood of confusion, the court noted that the two AltaVista marks are similar, that both companies, for relevant purposes, were supplying the same service, that both companies were competing and advertising in some of the same markets, that there was some actual confusion on the part of third parties, that ATI's use of the AltaVista mark was intended to capitalize on Digital's mark, and that the AltaVista mark is a strong suggestive mark entitled to strong protection.[663]

The number of domain name conflicts have been rising sharply as more businesses move on-line. Some have involved companies in different lines of business that have coveted the same domain name.[664] Others have involved companies that are related to another rightful user of a domain name but that do not have appropriate permission to use a particular mark as a domain name.[665] Still others involve organizations that are trying to trade off of another's mark,[666]

---

662. *Id.* at 478.

663. *Id.* at 477-78.

664. *See, e.g.*, Interstellar Starship Services, Ltd. v. Epix, Inc., 983 F. Supp. 1331 (D. Or. 1997) (finding that a web page promoting a theater group was not likely to confuse people looking for a web site for circuit analysis); Juno Online Services, L.P. v. Juno Lighting, Inc., 979 F. Supp. 684 (N.D. Ill. 1997) (finding no trademark misuse or state law deceptive business practices); Teletech Customer Care Management (California), Inc. v. Tele-Tech Company, Inc., 977 F. Supp. at 1407, (C.D. Cal. 1997) (engineering and installation contractor's use of "customer care" company's trademark as a domain name is likely to produce confusion, especially since contractor's name is available as a domain name, but is not being used by contractor). *Cf.* Lockheed Martin Corp. v. Network Solutions, Inc., 985 F. Supp. 949 (C.D. Cal. 1997) (noting that mere registration of a domain name which matches another's trademark is not sufficient to find infringement of the mark).

665. Travel Impressions Ltd. v. Kaufman. No. 96 CV 4503 (JG), (E.D.N.Y. May 22, 1997) (finding franchisee registered franchiser's mark as a domain name in excess of franchisee's authority provided in franchise agreement).

666. *See, e.g.*, Toys "R" Us v. Akkaoui, No. C 96-3381, 1996 WL 772709, (N.D. Cal. Oct. 29, 1996), (finding "adultsrus.com" domain name is likely to dilute Toys "R" Us family of trademarks).

or are otherwise trying to divert attempts at finding the mark-holder's Internet address.[667]

Some of the more interesting trademark cases have involved "domain name squatting," where someone registers the domain name that matches a company's trademark in the hope of selling the name to the company at a profit. Many of these cases have involved Dennis Toeppen, who runs an Internet service provider business in Illinois. Although many of the domain names for which he has registered are for his legitimate service provider clients, he has registered some because he "felt it would be interesting to see how the world responded."[668] The "world" responded by filing several lawsuits.[669]

One suit was a result of Toeppen's registering the domain "intermatic.com," which he used to put up a web page with an aerial map of Urbana, Illinois.[670] Another suit resulted from his registering "panavision.com" (and then later "panaflex.com").[671] After registering the "panavision.com" domain name, Mr. Toeppen set up a web page at the domain to display aerial photographs of Pana, Illinois. He did not use any of the Panavision domains to sell any goods or services.[672]

The *Intermatic, Inc.* (Intermatic) court applied the Seventh Circuit's likelihood of confusion test and found that there was enough of a question as to likelihood of confusion to survive a motion for summary judgment.[673] In contrast, the *Panavision International, L.P.* (*Panavision*) court held that Toeppen's use of the mark constituted dilution (and therefore did not determine if there was any likelihood of confusion).[674] Additionally, the *Intermatic* court found that Toeppen's registration prevented Intermatic from using its mark as its

---

667. Planned Parenthood Federation of America, Inc., v. Bucci, 1997 WL 133313, (S.D.N.Y. Mar. 24, 1997) (holding defendant's registration of "plannedparenthood.com" domain name to divert people seeking plaintiff's web site and to peddle antiabortion books infringes plaintiff's trademark).

668. Dennis Toeppen, Usenet News Post to the group chi.internet, message ID dennis-2611960911580001@victorville-34.net66.com, Nov. 6, 1996.

669. Panavision Int'l, L.P. v. Toeppen, 945 F. Supp. 1296 (C.D. Cal. 1996); Intermatic, Inc. v. Toeppen, 947 F. Supp. 1227 (N.D. Ill. 1996); American Standard Inc. v. Toeppen, No. 96-2147, 1996 U.S. Dist. LEXIS 14451 (C.D. Ill. Sept. 3, 1996).

670. *Intermatic, Inc.*, 947 F. Supp. at 1232-33. Eventually this map was moved, and the only thing appearing at the www.intermatic.com address was a notice that the Champaign-Urbana map page had moved to a new address. *Id.*

671. *Panavision Int'l, L.P.*, 945 F. Supp at 1298.

672. *Id.* When Panavision came asking for the domain name, Toeppen offered to transfer it to the company in exchange for $13,000. Panavision sued instead.

673. 947 F. Supp. at 1236.

674. 945 F. Supp at 1304.

domain name, but the court at least acknowledged that Intermatic could still possibly use its mark *in* its domain name.[675] This finding was unlike that in *Panavision* where the court (erroneously) argued that because Toeppen reserved the Panavision name, he foreclosed Panavision's ability to identify its goods on the Internet, and thus diluted Panavision's mark.[676]

Both courts held that this prevention of the rightful owner's using the mark as a domain name constituted dilution.[677] This conclusion is arguably incorrect; merely registering a name is not a use of the name in the trademark sense.[678] It does not make it any less likely that a consumer will think that a Panavision or Intermatic product came from Panavision or Intermatic. In essence, there is no dilution.[679] Interestingly, Judge Pregerson, who decided the *Panavision* case, has attempted to clarify this point in *Lockheed Martin Corp. v. Network Solutions, Inc.* by holding that merely registering a domain name is not necessarily an infringement of a matching trademark.[680]

To the court's credit, Toeppen did more than just register the domain names. He also set up web pages at all of the domains. When Toeppen set up the web page, even to display the map of Pana or Urbana, he provided something which could be attributed to the mark holder. However, the Dilution Act requires not just a use of the mark, but a "commercial use in commerce" of the mark.[681] The courts found this requirement met not because of the web page, but because of Toeppen's efforts to sell the domain name.[682] For instance, Judge Pregerson in *Panavision* stated:

---

675. *Intermatic, Inc.*, 947 F. Supp. at 1232-34.

676. *Panavision, Int'l, L.P.*, 945 F. Supp. at 1304.

677. *Intermatic, Inc.* 947 F. Supp. at 1240; *Panavision, Int'l*, 945 F. Supp. at 1304.

678. *See* Lockheed Martin Corp. v. Network Solutions, Inc., 985 F. Supp. 949, 957 (C.D. Cal. 1997). *Cf.* La Societe Anonyme des Parfums Le Galion v. Jean Patou, Inc., 495 F.2d 1265, 1273 (2d Cir. 1974) (noting "warehousing" of name by token use was not sufficient use in commerce to reserve rights in name); Marvel Comics, Ltd. v. Defiant, a Division of Enlightened Entertainment, Ltd., 837 F. Supp. 546, 548 (S.D.N.Y. 1993) (noting certain preregistration use were adequate uses in commerce for trademark purposes); Societe De Developments Et D'Innovations Des Marches Agricoles Et Alimentares-Sodima-Union De Cooperatives Agricoles v. Int'l Yogurt Co., Inc., 662 F. Supp. 839, 852 (D. Or. 1987) (stating token use of a product for purpose of reserving name is not an adequate use for trademark purposes).

679. This holding conflicts with the result in Actmedia, Inc. v. Active Media Int'l, Inc., No. 96C 3448, 1996 WL 466527 (N.D. Ill. July 17, 1996), where the court held that merely reserving a domain name violates 15 U.S.C. § 1125 (West Supp. 1998) and Illinois Common Law.

680. 985 F. Supp. 949, 957 (C.D. Cal. 1997).

681. *See* 15 U.S.C. § 1125(c)(1).

682. *Panavision Int'l, L.P.*, 945 F. Supp. at 1303; *Intermatic, Inc.*, 947 F. Supp. at 1239-40.

> In the case before the Court, however, Toeppen has made commercial use of the Panavision marks. Toeppen's "business" is to register trademarks as domain names and then to sell the domain names to the trademarks' owners. Toeppen's business is evident from his conduct with regard to Panavision and his conduct in registering the domain names of many other companies. His "business" is premised on the desire of the companies to use their trademarks as domain names and the calculation that it will be cheaper to pay him than to sue him.[683]

Despite the courts' assertions, even registering a domain name and offering it for sale does not match the definition of a use in commerce as defined in the Lanham Act.[684] The Act defines a use in commerce as follows:

> The term "use in Commerce" means the bona fide use of a mark in the ordinary course of trade, and not made merely to reserve a right in the mark. For purposes of this chapter, a mark shall be deemed to be in use in commerce—
> (1) on goods when—
>
> > (A) it is placed in any manner on the goods or their containers or the displays associated therewith or on the tags or labels affixed thereto, or if the nature of the goods makes such placement impracticable, then on documents associated with the goods or their sale, and
> > (B) the goods are sold or transported in commerce, and
>
> (2) on services when it is used or displayed in the sale or advertising of services and the services are rendered in more than one State . . . and the person rendering the services is engaged in commerce in connection with the services.[685]

Courts have held that merely registering a name in order to reserve a right to the name is not sufficient use in commerce. The mark must be applied to an identifiable product with an intent to

683. *Id. See also Intermatic, Inc.*, 947 F. Supp. at 1239-40 (stating "Toeppen's intention to arbitrage the 'intermatic.com' domain name constitutes a commercial use . . . Toeppen's desire to resell the domain name is sufficient to meet the 'commercial use' requirements of the Lanham Act.").

684. *Panavision Int'l, L.P.*, 945 F. Supp. at 1304. "In addition, the Dilution Act itself excepts certain uses and thereby protects parties who 'innocently' register a famous trademark as a domain name (e.g., a citizen of Pana, Illinois who registers 'panavision.com' in order to provide a community political forum would come under the exemption for non-commercial use)." *Id.*

685. 15 U.S.C. § 1127 (West Supp. 1996).

distribute that product.[686] Toeppen's attempt to get money from Panavision and Intermatic by selling them the like-named domains he had registered was not a public use of those names to identify the source of goods or services.[687] If anything, the domain names were Toeppen's goods, rather than merely a label he was using as a source identifier for his trademark-speculating services. The level of confusion injected into trademark law is illustrated clearly in the *Lockheed-Martin v. Network Solutions, Inc.* case. This case addressed the issue of the registrar's liability for allowing third parties to register domain names which may be confusingly similar to another's trademark. Judge Pregerson stated that he found the defendant liable in the *Panavision* case because he not only registered a domain name, but he also offered to sell it to the plaintiff because it had value to Panavision because the domain name matched its trademark.[688] In *Lockheed-Martin,* the court held that the defendant was not liable for trademark infringement even though it is in the business of registering domain names and even though it particularly hopes to realize the value of selling domain names that match trademarks to trademark owners.[689] The distinction Judge Pregersonnn draws is that Network Solutions, Inc. is only involved with the "technical function" of a domain name—matching a name to its underlying address. In other words, Network Solutions, Inc. is not liable because it does not use the domain names as trademarks, it merely registers them and sells them to trademark holders. However, Judge Pregerson summarized his holding in *Panavision* by stating that "[t]his decision merely holds that registering a famous mark as a domain name for the purpose of trading on the value of the mark by selling the domain name to the trademark owner violates the federal and state dilution statutes."[690] In both cases, the courts reached the "just" conclusion. It seems clear,

---

686. *See, e.g., International Yogurt Co., Inc.*, 662 F. Supp. at 852; *Lockheed Martin Corp.*, 985 F. Supp. at 957.

687. *Marvel Comics, Ltd.*, 837 F. Supp. at 548. "As for sufficient 'use in commerce,' the 'talismanic test' is whether or not the use was 'sufficiently public to identify or distinguish the marked goods in an appropriate segment of the public mind as those of the adopter of the mark." *Id. See also Jean Patou, Inc.*, 495 F.2d at 1274.

> Trademark rights are not created by sporadic, casual, and nominal shipment of goods bearing a mark. There must be a trade in the goods sold under the mark or at least an active and public attempt to establish such a trade . . . Registerable rights manifestly cannot flow from these activities and the old adage 'no trade—no trademark' is applicable here.

Id.

688. 985 F. Supp. at 957.

689. *Id.*

690. *Panavision Int'l, L.P.*, 945 F. Supp. at 1300.

however, that they are contradictory, and therefore one of the opinions must be incorrect.

Another creative analysis was applied to the domain name issue in *Planned Parenthood Federation of America, Inc. v. Bucci*.[691] In that case, Judge Wood held that because of the interstate nature of the Internet in general, which requires the use of long distance phone lines to access a remote web page, and because of the fact that the activities of a multistate business were blocked by the defendant's use of a plaintiff's mark as a domain name, the "in commerce" requirements of the Lanham Act were met.[692] This is arguably false for the same reason it is false in the *Panavision* and *Intermatic* cases. Judge Wood seems to be breaking a phrase defined by the statute into two parts ("commercial use" and "in commerce") and analyzing the sections separately, rather than as the term of art defined in the statute.

However, more interestingly, Judge Wood points out that Section 32 of the Lanham Act does not contain an "in commerce" requirement.[693] This section of the Act prohibits the use of a mark, without permission, "in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive."[694] Judge Wood held that "informational services" can fall under this definition, and if the information provided is likely to lead "[p]rospective users of plaintiff's services who mistakenly access defendant's web site [to] fail to continue to search for plaintiff's own home page, due to anger, frustration, or the belief that the plaintiff's home page does not exist" there may be a remedy under Section 32.[695] Notably, Judge Wood held that the defendant's acts in the *Planned Parenthood* case constituted a commercial use of the mark. The defendant had set up an antiabortion web page at "plannedparenthood.com" in order to intercept people intending to find the plaintiff's family planning site. Judge Wood stated:

> [D]efendant's use is commercial because of its effect on plaintiff's activities. First, defendant has appropriated plaintiff's mark in order to reach an audience of Internet users who want to reach plaintiff's services and viewpoint, intercepting them and misleading them in an attempt to offer his own political message. Second, defendant's appropriation not only provides Internet users with competing and

691. No. 97 Civ. 0629, 1997 WL 133313 (S.D.N.Y. Mar. 24, 1997).
692. *Id.* at *3.
693. *Planned Parenthood Education of America*, 1997 WL 133313 at *4.
694. *Id.*
695. *Id.*

> directly opposing information, but also prevents those users from reaching plaintiff and its services and message. In that way, defendant's use is classically competitive: he has taken plaintiff's mark as his own in order to purvey his Internet services—his web site—to an audience intending to access plaintiff's services.[696]

One case has applied a trademark analysis to Internet addressing in a nondomain name context. The court in *Patmont Motor Werks, Inc. v. Gateway Marine, Inc.*, held that using a trademark in a web site address following the domain name—in this case using the GO PED trademark in the address <http://www.idosync.com/goped>—could not constitute an infringement.[697] Additionally, the court stated that while use of a trademark in a domain name may allow for confusion as to sponsorship, use after the domain name could not produce confusion as to sponsorship.[698]

As a blanket statement, this holding is clearly erroneous. It is not uncommon for a trademark owner to set up a web site on a service provider's machine without obtaining a separate domain name (as was the situation in the *Patmont* case). Also, a merchant who sets up shop in an on-line shopping mall may have an address such as <http://www.shoppingmall.com/trademark>. Clearly such a use could involve an indication of sponsorship, and thus clearly such a use, with the right set of facts, could constitute a trademark infringement.

New methods of taking advantage of the goodwill developed by others are continually being developed. For example, Playboy Enterprises has obtained an injunction against a Web site trying to capitalize on the Playboy mark.[699] A preliminary injunction was entered prohibiting the defendant from using its playboyxxx.com or playmatelive.com domain names.[700] Importantly, however, the court also enjoined the use of Playboy's trademarks in the "meta-tags" of the defendant's Web pages. "Meta-tags" are elements of computer code normally hidden from the view of people looking at Web pages. Search engines,[701] however, read the key words a web site designer puts in this hidden code for rating how closely a web page's content

696. *Id.* at *6.
697. No. 96-2703 1997 WL 811770, at *3 and *4.
698. *Id.* at *4.
699. Playboy Enterprises, Inc. v. Calvin Designer Label, 985 F. Supp. 1220 (N.D. Cal. 1997).
700. *Id.* at 1225.
701. Search engines are databases available via the Web which indexes the content of other web sites thus allowing users to search for web pages which (might) contain material of interest to them.

matches the search request of a search engine user looking for specific content. Thus by manipulating the content of the meta-tags, a web site designer can affect what searches will provide a reference to the web page and the prominence the page will receive in a search report.[702] In this case, the defendants had embedded Playboy's trademarks in the meta-tags of their playboyxxx.com and platmatelive.com sites so that Internet users searching for the plaintiff's web site as well (or instead). Playboy has also obtained a victory against AsiaFocus International claiming the defendant's use of Playboy trademarks in the meta-tags constitute trademark dilution.[703]

Playboy Enterprises is not the only party seeking relief due to others' inappropriate use of trademark in meta-tags. Insituform Technologies, Inc. received a consent judgment against National Envirotech Group prohibiting the defendant from using the plaintiff's marks in the defendant's web page, but also requiring the defendants send letters to some of the major search engines asking them to ensure that a new version of the defendant's web site—which no longer contains the confusing meta-tags—is listed in their databases instead of the original pages.[704]

Not all meta-tag cases have been resolved immediately in the plaintiff's favor. In *Playboy Enterprises, Inc. v. Wells*, the court held that a former Playmate of the Year, Terri Wells, was entitled to use certain trademarks belonging to Playboy Enterprises.[705] The court denied the plaintiff's motion for summary judgment because Ms. Wells had been a Playboy Playmate and had been Playmate of the Year and had been specifically allowed to refer to herself as having won these titles from Playboy Enterprises. Thus, the court stated, her use of the marks was fair in the same way and Academy Award winner could state that he or she had won an Oscar or a Heisman Trophy winner could refer to having won the award.[706] The court allowed this "fair use" argument to extend to the use of Playboy marks in the meta-tags on Ms. Wells' web site, in part perhaps because of the otherwise noninfringing nature of the web site.

702. A term often used for such manipulation of search engine results, often by reporting key words multiple times in a web page's meta-tags or otherwise hiding such text, is "spamdexing."

703. *See* C/Netnews.com, discussing *Playboy Enterprises, Inc. v. AsiaFocus International*, visited June 10, 1998 <http://www.news.com/News/item/0,4,21370.html>.

704. Insituform Technologies, Inc. v. National Envirotech Group, L.L.C., No. 97-2064 (E.D. La. Aug. 27, 1997) (on file with the *Seattle University Law Review*).

705. No. 98-CV-0413 (S.D. Cal. Apr. 21, 1998) (on file with the *Seattle University Law Review*).

706. *Id.*

XI. CONCLUSION

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[707] and the Electronic Frontier Foundation.[708] 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 U.S. Constitution to protect individuals from such violations of their rights. His proposed amendment reads:

> This Constitution's protections for the freedoms of speech, press, petition, and assembly, and its protections against unreasonable searches and seizures and the deprivation of life, liberty, or property without due process of law, shall be construed as fully applicable without regard to the technological method or medium through which information content is generated, stored, altered, transmitted, or controlled.[709]

This amendment would serve to ensure that the speech and privacy rights that we currently enjoy in other media would be applied to electronic communications as well. An amendment such as this would hopefully 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. This is particularly important as electronic publishing and electronic document delivery become the norm, rather than the exception.[710]

---

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

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

709. *Laurence Tribe Proposed Constitutional Amendment, available over* INTERNET, by anonymous FTP, at FTP.EFG.ORG (Electronic Frontier Foundation) (visited March 29, 1998).

710. *See generally* John Browning, *Libraries Without Walls for Books Without Pages*, WIRED, 1.1, Premiere Issue, 1993, at 65 (discussing the Bibliotheque de France's digital scanning of "100,000 great works of the 20th century as chosen by a committee of notable French

What is necessary to regulate computer information system content and system operator liability is, first and foremost, an understanding of the technology. The law is a slow-evolving, tradition-bound beast. Computers are an upstart technology pioneered by people who do things like create viruses to let loose on their friends in order to hone their programming skills.[711] If judges, juries, lawyers, and legislators do not understand current technology, the technology will change 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[712] works well to regulate electronic mail because it is modeled after the statute that governs the U.S. mail.[713] For many people, these new communications fora are direct replacements for old means of communications; 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 user's point of view. At some point, totally new models of regulation may be appropriate.

Where novel legislation is needed is in defining terms to be used in the developing law and in filling any gaps. One illustration 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? Another example is the copying of electronic documents. Should merely reading an electronic text into RAM constitute a potentially infringing copy? How does a library lend an electronic document without making a copy?

Tribe's proposed constitutional amendment is rooted in logic similar to underlying logic of a natural law concept. Because constitutional protection already exists, 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 systems grow in their use, older media will pass away. The growth of computer networks and

citizens").

711. *See* Branscomb, *supra* note 408, at 7-11.

712. 18 U.S.C. § 2511 (1994).

713. 18 U.S.C. § 1702 (1994).

on-line services in the past few years has been explosive. New laws will have to be added, and old laws will have to evolve to conform with the specific demands of the new media.

A growing imperative will also be international coordination of laws. "The point is that pretty soon you'll have no more idea of what computer you are using than you have of where your electricity is generated when you turn on the light."[714] For a networked computer, access can be had from anywhere there is a network connection. Often, there is little or no easy way to determine in which state or country the computer you are using is located. In our interconnected society, there may not even be a clear way to establish which sovereign's laws will apply. International cooperation will become essential in resolving matters such as conflicts of laws if the legal environment is to be truly clear and understandable to guide the behavior of system operators. In cases where the law will not provide clarity, some network users will resort to "self help" remedies to perceived ills—hacking the hackers until a sort of "justice" is achieved.

714. Danny Hillis, *Kay + Hillis* , WIRED, 2.01, Jan. 1994, at 103.