

ARTICLE***Liabilities of System Operators on THE Internet******Giorgio Bovenzi*** †**TABLE OF CONTENTS****I. INTRODUCTION****II. NETWORK PROVIDERS POTENTIALLY LIABLE FOR THE TORTS OF THEIR USERS**

A. The Internet and Internet Service Providers

B. Commercial On-line Services

C. Bulletin Board Systems

III. PRIVACY

A. The Right to Privacy

B. Privacy, the "Right of the People Peaceably to Assemble" and Anonymity

C. Relevant Federal Statutes

D. Traditional Mail v. E-Mail

E. Conclusion

IV. FLAMING

A. Defamation

B. *Cubby v. CompuServe*C. *Stratton Oakmont, Inc. v. Prodigy Services Co.*D. *Religious Technology Center v. Netcom On-line Communication Services, Inc.*

E. Analogies for Sysop's Liability

F. Sysop's Liability: A Tentative Conclusion

V. COMPUTER SYSTEMS, PUBLIC FORA AND POLICIES**VI. CONCLUSION****I. Introduction**

In the thirteenth century, Emperor Frederick II proclaimed instruments written on paper to be invalid.¹ Despite resistance from the legal community, however, paper was eventually deemed to be dignified enough to replace parchment in legal use.² Centuries later, typewriters made handwritten documents obsolete, although lawyers realized that they made forgery much simpler.³

Time and again, technologically new ways of conducting business encounter initial resistance, but ultimately are embraced by the common law. The law ultimately seeks fairness and ease of trade, preferring the substance of a transaction over its form. Attorneys sense, with good reason, that the law will track technological changes, and they gladly put new technology to use.

Today, the choice of the medium through which a transaction is executed affects the negotiation process. Often, the methods successfully employed in one case might be ineffective in another.⁴ Rather than dismissing electronic transactions just because the controls are imperfect,⁵ lawyers must acquire new skills to negotiate effectively in the electronic world. It is no longer true that everything that can be done in cyberspace can be done in the physical world as well. In fact, the low cost and high speed of electronic activities, and the sophisticated interaction of communication media, have fundamentally changed the parameters, goals and accomplishments of the participants.⁶

Communications is an area of technology where this is especially true. The exploding usage of electronic communications, notably through the Internet, offers an amazing opportunity to expand communications capabilities and opportunities. But like all new technologies, such communications raise both novel questions of law and traditional questions of law in novel settings. The application of old-style laws to this new-style medium may deter the expansion of the Internet.

One important example is the liability of Internet system operators for torts committed through the medium they provide. The users of an electronic means of communication are certainly liable for any torts—such as invasion of privacy and defamation—they commit on line.⁷ What is not clear is whether system operators who form part of the causal link in the user's tort should be held liable as well.⁸ If someone illegally accesses a user's mailbox, for example, should the system operator be held liable for allowing access to private data? Similarly, should the system operator be liable for defamation based on a failure to control or to remove the defaming information from the system? The chain of events and actions that connect the user's injury to the system operator's conduct might be long and sinuous.⁹ Nevertheless, the tort goals of deterrence and victim compensation indicate that, in general, liability may follow.¹⁰ The answer will depend in part on the traditional law regulating defamation or invasion of privacy, as applied in this new setting. But the answer should also take into consideration the related interests of encouraging the growth of the Internet and of protecting freedom of speech. This article suggests a framework for legal analysis which will minimize deterrence of electronic communication while still providing protection for individual users of the Internet.

The article begins with a discussion of computer networks, system operators and the activities offered on-line. Next it demonstrates that the rights to privacy and to assembly exist in on-line activities, and explores the implications of these rights for Internet users. The discussion continues with an overview of defamation as manifested on line. The article then analogizes computer networks to other communication media in order to propose a tentative framework for determining system operators' liabilities for harmful messages posted on their systems.¹¹ Finally, the article draws upon the public forum doctrine to develop policies which should guide future regulation of the electronic communication industry.

II. Network Providers Potentially Liable for the Torts of their Users

The right of an injured party to seek damages from the tortfeasor is not controversial. An individual user who commits torts such as reading private e-mail or publishing a defamatory or obscene message will surely be held liable. Controversy continues, however, over the level to which the system operator can also be held liable when a user commits such torts. System operators (sysops) must know the legal risks they face in running a computer system. Otherwise, they may be embroiled in avoidable litigation, or, fearing liability, they may unnecessarily restrict access to the services they provide.

The extent of potential liability varies from case to case. In large part, it will depend on the extent of the editorial control exercised by the sysop. This is often determined by the structure of the service through which the tort is committed. Thus, we must distinguish between several types of networks: the Internet, commercial on-line services and private bulletin board systems (BBSs). While these systems are structured somewhat differently, ultimately each poses similar questions of liability. In each case, a sysop provides the medium for electronic communication. Depending on the facts of each case, these sysops may be held liable for the torts of users.

A. The Internet and Internet Service Providers

The Internet is a network of networks.¹² Many computers connected together create a system, and many systems connected together

create a network. Thousands of local networks connect in a sort of spider's web in which communication software called Transmission Control Protocol/Internet Protocol (TCP/IP) manages communications between computers.¹³ The user perceives the system to be a unique, uniform network: the Internet.¹⁴ Interestingly, the Internet is decentralized, with no central hub through which all messages must be routed and no central governing entity. Still, this anarchic autonomy has proven, so far, to be surprisingly effective.

Originally intended for users at universities and in the military, in recent years the Internet has become popular with users of all sorts.¹⁵ Many of them access it through companies known as Internet service providers (ISPs), such as Netcom, or through service provided by their employers or universities. Customers dial in to a computer run by the ISP; this computer is linked to the Internet.¹⁶ In the decentralized Internet system, these ISPs are the "system operators," potentially liable for the on-line torts of those to whom they provide access.

B. Commercial On-line Services

Before the Internet became widely available, commercial on-line services like Prodigy, CompuServe and America Online were the primary means of electronic communication for most computer users.¹⁷ These private networks offer various on-line activities through their own mainframe computers. Originally, these on-line services were not linked to the Internet; as the Internet became more popular, however, they expanded their services to offer such links.¹⁸ These services could be held liable as sysops for the on-line torts of their customers either within their own system or, like the ISPs, for torts committed on the Internet through the gateway they provide.

Though organization and nomenclature may vary from company to company, both ISPs and commercial service providers typically offer a combination of services including e-mail and public messaging services, software collections, recreational forums and electronic publication libraries. To participate in discussions of a particular topic, a user can subscribe to a mail list, and then receive a copy of every message sent to the list; read messages publicly posted on an electronic bulletin board; or join a newsgroup. Another kind of electronic discussion is offered by the "chat" feature, which allows a live computer-to-computer conversation in which several users can type their messages to each other. More advanced systems create "private rooms" where users have intimate conversations. In addition to these features, commercial on-line services offer discussion forums on a wide range of topics, electronic versions of magazines and information services, stock quotations and news services and so on.

C. Bulletin Board Systems

A third type of electronic communications system is the computer bulletin board system (BBS). In many ways, these are similar to the commercial on-line services, except they are often free of charge.¹⁹ Since BBSs are easily set up on small personal computers with a single phone line, special interest BBSs, often run by computer hobbyists, are common.²⁰ Though some BBSs are connected to the Internet, many are strictly private, accessible only by users to whom the sysop distributes the phone number. Information on a BBS is typically organized in directories. Users can dial in directly to the host computer and access this information. In addition, users can read and post messages on the BBS. The operators of those BBSs associated with the Internet have created USENET, a system by which the messages posted on local USENET-site BBSs are organized into topical newsgroups and distributed to Internet sites.²¹ Like a commercial on-line service, the sysop of a BBS could be held liable for torts committed within the BBS itself. If a defamatory message is posted through USENET to the much wider Internet newsgroup audience, the sysop could be liable for that as well.²²

One of the important differences between commercial on-line services and BBSs is that the activity on the BBSs is often moderated by the sysop, who receives the messages and decides which ones to post to a given newsgroup.²³ The sysop screens off messages that are not topical or otherwise unacceptable. This distinction is crucial, since the amount of editorial control exercised by a sysop becomes the key factor in ascertaining the sysop's liability for users' torts.

The above is an overview of the types of communication taking place on line and the different types of services available to the user. The following sections will discuss in more detail two torts frequently encountered on line, violation of privacy and defamation, and will analyze the probable duties of sysops with respect to each.

III. Privacy

Account holders have the right to expect that their on-line affairs, such as personal information or confidential business information, will be private. Users who intrude into the affairs or identity of others are liable for invasion of privacy; the sysop who allows such intrusion to occur may be liable as well. One important aspect of the right to privacy is the right to anonymity, a crucial component of the constitutional right to communicate and to peaceably assemble.²⁴ A sysop should be able to refuse to reveal users' identities to the

government absent a compelling state interest.

Factors in a court's decision of liability for invasion of privacy will include common law doctrines related to invasion of privacy, but will also include some applicable federal statutes. A useful analogy, which may provide a good basis for future analysis, is to compare the role of a network service provider with the role of the United States Post Office, which bears a legal duty to prevent offensive mail from reaching a customer who has complained.

A. The Right to Privacy

The common law of privacy affords a tort action for damages resulting from an unlawful invasion of privacy.²⁵ For example, an intrusion upon the plaintiff's seclusion or solitude, or into his private affairs, constitutes the tort of invasion of privacy.²⁶ This should hold true on line as well as in the physical world. Sysops may face liability if they enable someone to intrude wrongfully in the private affairs of a user or account holder on their system. Sysops who give third parties access levels that facilitate illicit prying into private areas might be found liable as well.

The tort of violation of privacy developed from the law of trespass to land,²⁷ but it also extends to cases in which there is no entry into the plaintiff's premises at all: for example, peering through windows,²⁸ reading someone's private correspondence,²⁹ overhearing conversations by means of a parabolic microphone,³⁰ and surreptitiously gaining access to someone's data or files³¹ all constitute invasions of privacy. For this purpose, there is no valid distinction between files physically kept in an office and those kept on a computer. Indeed, owing to their superior record keeping and transmission capabilities, computer systems heighten the risks involved with invasion of privacy issues. Record keepers can collect and store more information than in the days of paper records. Confidential information stored in computer networks may include privileged communications such as those between an attorney and client or related work-product materials. All these materials must remain confidential.³²

Yet the information is more easily accessed in computer format than on paper. In fact, the information in a computer database is organized to make sorting and retrieval as convenient as possible, and the nature of databases implies that multiple users can access the data. Placing privileged and confidential business information in databases raises the question as to whether the ease of accessibility to the databases acts as a practical waiver of the privileged status of confidential information.

There are many different ways for a sysop to ensure the security of a system containing confidential information. The sysop should eliminate any inactive accounts. Next, the sysop could install password-screening programs which require users to choose only passwords which are not easily guessed. Cryptography may be used to guarantee that private communications remain secret. Each message may be encoded so that it cannot be deciphered without the original algorithmic key.³³ Nearly everything in cyberspace could be encrypted. No one, including the government, can easily decrypt messages encrypted with some of today's advanced cryptographic tools.³⁴ The sysop should post the rules regarding whatever security systems are in place, and ensure that these rules are enforced. These actions should constitute reasonable steps taken to protect the privacy of the system users.

The concept of privacy is a fluid one and new forms or concepts of privacy may be recognized.³⁵ The custom of the time and place forms the basis for determining what is private. Ultimately, privacy is a subjective matter, the bounds of which depend on social norms that can change. In a world that fosters the application of new technologies to usual activities and transactions, the introduction of new concepts of privacy, adapted to protect new interests, may render the new forms of communication less intrusive and more acceptable.

B. Privacy, the "Right of the People Peaceably to Assemble" and Anonymity

Anonymity is an important element of the right of privacy and the related constitutional right to peaceably assemble.³⁶ Anonymous authorship can sometimes achieve more constructive purposes than attributed publication. Alexander Hamilton, James Madison and John Jay, for example, published the *Federalist Papers* under the pseudonym "Publius."

In *Talley v. California*,³⁷ the Supreme Court held void on its face a city ordinance restricting distribution of "any hand-bill, in any place under any circumstances, which does not have printed on the cover . . . the name and address of the . . . person who printed, wrote, compiled or manufactured the same . . . [or] caused the same to be distributed."³⁸ Justice Black wrote for the Court that "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance."³⁹ Recently, in *McIntyre v. Ohio Elections Commission*,⁴⁰ the Supreme Court struck down a similar ban as conflicting with the "honorable tradition" of anonymous pamphleteering in U.S. history and the need to prevent retaliation against people who want to disseminate controversial views.⁴¹ Thus, it can be said that the protection of anonymity is rooted in both freedom of speech and the right to privacy.

In *NAACP v. State of Alabama*,⁴² the Court commented on the issue of the privacy of a group's records, noting that "[i]nviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."⁴³

Five years later, the Supreme Court offered a more complete examination of the protection afforded associations by the constitutional right to assemble. In *Gibson v. Florida Legislative Investigation Committee*,⁴⁴ the Court upheld the right of the NAACP to deny the government access to its membership lists on the basis of its right of association "when such disclosure will seriously inhibit or impair the exercise of constitutional rights and has not itself been demonstrated to bear a crucial relation to a proper governmental interest or to be essential to fulfillment of a proper governmental purpose."⁴⁵ Freedom to engage in association is an inseparable aspect of the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech. Therefore, when a state's demand constitutes a significant encroachment on personal liberty, the state may enforce disclosure only on a showing of a compelling interest.⁴⁶

The Internet offers a practical opportunity for assembling and communicating in anonymity. A user who wants to keep his e-mail messages anonymous can route them through systems known as anonymous servers, which strip a message of any information identifying the sender, assign it an identification code, and deliver it to the intended recipient.⁴⁷ In spite of their popularity, anonymous servers cannot guarantee absolute anonymity. The information traffic on the system might still be monitored or logged by the sysop, or by illegal hackers. Analogous monitoring is possible in the case of an anonymous file transfer through Internet File Transfer Protocol (FTP).

The identities of people using certain services or advocating certain views through "anonymous" e-mail might well be of interest to the government; but the First Amendment should allow and perhaps require sysops to withhold that information. Thus, sysops should be able to prevent the government from accessing all of the information contained in their user records.⁴⁸ Like the anonymous pamphleteers and the NAACP members, their identities would seem to be protected by the twin rights of privacy and of assembly. Unauthorized release of such information may entitle the injured individual to recover from the sysop in such situations.

C. Relevant Federal Statutes

Statutes, as well as the common law, may regulate the liability of sysops for invasions of privacy on their systems. Three statutes which bear on this issue are the Electronic Communications Privacy Act of 1986,⁴⁹ which allows sysops to intercept and disclose information in some situations and requires disclosure in others; the Communications Assistance for Law Enforcement Act of 1994,⁵⁰ which expands privacy and security protection for telephone and computer communication, including protection of e-mail addresses; and the Communications Decency Act of 1996,⁵¹ which prohibits sending or displaying indecent communications to minors, and introduces new defenses for access providers who do not create the offensive content.⁵²

As mentioned above, the legal community faces privacy problems when dealing with attorney-client privileged materials transferred on line. Issues of discovery and evidence are also likely to arise. While legislation has begun to adapt to the new necessities, the technology and the costs required to make it effective may be still prohibitive, and the implementation of security systems slows down the flow of data.

1. The Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act of 1986 (ECPA), an update of a 1968 law regulating wiretapping,⁵³ prohibits intercepting, disclosing or divulging private communications. The law's coverage specifically includes electronic communications.⁵⁴ Damages are available to anyone harmed by a violation of the Act.⁵⁵ Appropriate types of relief include preliminary, equitable or declaratory relief, damages as specified in particular circumstances, punitive damages in appropriate cases and reasonable attorney's fees together with litigation costs.⁵⁶

Sysops are the beneficiaries of several specific exceptions to the Act's broad prohibition. A system operator, in fact, may use random monitoring for quality control checks, and can intercept, disclose or use communications in the normal course of his business "while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service."⁵⁷ At the same time, sysops are also "authorized to provide information, facilities and technical assistance to persons authorized by law to intercept [such communication] or to conduct electronic surveillance."⁵⁸ Another exemption allows sysops to use a pen register or a trap-and-trace device, or "to record the fact that a wire or electronic communication was initiated or completed," if its purpose is to protect the sysop, another sysop or a user from "fraudulent, unlawful or abusive use of such service."⁵⁹ The Act also prohibits the sysop who provides a service to the public from intentionally divulging the contents of any communication while in transmission on that service to any person other than the addressee or the intended recipient of the communication,⁶⁰ except if

otherwise lawfully authorized or if the contents of the communication were inadvertently obtained and appear to pertain to the commission of a crime.⁶¹

Others who benefit from exemptions under the Act include officers, employees and agents of the Federal Communications Commission acting in the normal course of their duties.⁶² Also, the law does not apply when the person who intercepts is a party to the communication, or when one of the parties has given prior consent.⁶³

In Title II, the ECPA extends similar prohibitions on divulging the contents of communication while it is stored. Persons or entities providing an electronic communication service or a remote computing service to the public cannot knowingly divulge the communication which is in electronic storage or which is carried or maintained on that service on behalf of a subscriber (or a customer) and for purposes of storage.⁶⁴ The requirements for government access to stored and existing electronic communications are also spelled out. A governmental entity may require a sysop to disclose the contents of any electronic communications only upon following strict procedures.⁶⁵ The sysop is entitled to demand that the government meet such conditions, and may incur liabilities in cases of unlawful disclosure or violation of civil rights.⁶⁶ The sysop has, in general, the option of informing the customer of the government's request, unless the government obtains a court order to prevent disclosure of the request.⁶⁷

The result of this legislative approach is that every sysop now has the burden to make clear to all users what types of messages may be disclosed to others and what may not. While in some cases the law allows sysops to intercept, use and disclose private communications, in other cases the law specifically provides that sysops may be liable for unlawful disclosure.

2. The Communications Assistance for Law Enforcement Act of 1994

The purpose of the Communications Assistance for Law Enforcement Act of 1994 (CALEA)⁶⁸ is "to preserve the government's ability, pursuant to a court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes."⁶⁹ The Act imposes a duty to cooperate with law enforcement on telecommunications carriers.⁷⁰ These provisions, however, do not apply to information services or to equipment, facilities or services utilized by private networks.⁷¹

Some provisions in the Act are relevant to our discussion, however, because they expand privacy and security protection for telephone and computer communications not authorized to be intercepted. Specifically, the Act requires a court order rather than a subpoena to obtain e-mail addresses and other similar data from providers of electronic communications services;⁷² implies that the use of encryption is not to be limited;⁷³ and expands the privacy protections contained in the ECPA to cover cordless phones and data communications transmitted by radio.⁷⁴

The statute is also relevant to our discussion because Internet communications would likely be intercepted at the carrier that provides access to the public switched network.⁷⁵ Therefore, regulation of such carriers will have an impact, albeit indirect, on Internet communications.

Before it was enacted, this statute was accepted in principle by representatives of law enforcement agencies like the FBI, civil libertarian organizations like the Electronic Frontier Foundation, and the telephone industry.⁷⁶ The Committee on the Judiciary noted that the Act "seeks to balance three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy . . . and (3) to avoid impeding the development of new communications services and technologies."⁷⁷ The statute expands privacy and security protection for telecommunications carriers, and explicitly recognizes the right of subscribers and customers to use encryption.

3. The Communications Decency Act of 1996

The Communications Decency Act of 1996 (CDA),⁷⁸ which was included in the Telecommunications Act of 1996,⁷⁹ expands the Communications Act of 1934,⁸⁰ which covered only the telephone, to prohibit the use of *any* telecommunications device by persons who do not disclose their identity and have the intent to annoy, abuse, threaten or harass the recipient of such communication.⁸¹ The Act also prohibits the repeated use of a telecommunications device solely for harassment purposes.⁸² Additionally, the Act limits the old prohibition of "obscene, lewd, lascivious, filthy, or indecent" communication to cases when the communication is made with "intent to annoy, abuse, threaten, or harass,"⁸³ or, alternatively, "knowing that the recipient . . . is under 18 years of age."⁸⁴ Intentionally allowing another to use any telecommunications facility for such purposes is also punishable under the Act.⁸⁵ Violators of these provisions are subject to fines and/or a maximum sentence of two years in prison.⁸⁶

The most recent provisions, however, are those contained in the new subsections added to the Communications Act of 1934. These provisions are causing large debate and great controversy. The most controversial is the one that prohibits the use of, as well as granting permission to use, an interactive computer service⁸⁷ to send or display to a person under 18 years of age "communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs."⁸⁸ The person responsible for such violation can be fined and/or imprisoned for up to two years.⁸⁹ This new subsection codifies the definition of indecency approved in the Supreme Court case *FCC v. Pacifica Foundation*.⁹⁰ Both the House and the Senate Conference Reports indicate that the consideration of the *context* of the communication is crucial in ascertaining its offensiveness.⁹¹ "Material with serious redeeming value is quite obviously intended to edify and educate, not to offend."⁹²

The other subsection that has caused debate and controversy is the one that introduces new defenses for access providers, employers and good Samaritans, in addition to any other defenses already available at law. The "access provider" defenses exclude liability for persons who provide "access or connection to or from a facility, system, or network not under that person's control."⁹³ The exemption includes the provision of access "incidental to providing such access or connection that does not include the creation of the content of the communication."⁹⁴ Such defenses, however, do not apply "to a person who is a conspirator with an entity actively involved in the creation or knowing distribution of communication . . . or who knowingly advertises the availability of such communications."⁹⁵ Also, the defenses do not apply when the entity that provides access or connection is the owner of or otherwise controls the facility, system or network.⁹⁶ The "access provider" defenses are designed to limit the criminal penalties to content providers and conspirators, therefore excluding "entities that simply offer general access to the Internet and other on-line content. The conferees intend that this defense be construed broadly to avoid impairing the growth of on-line communications through a regime of vicarious liability."⁹⁷

The employer defense exempts employers from liability for their employee's or agent's actions, unless such actions are "within the scope of his or her employment or agency," and the employer has knowingly authorized or ratified, or recklessly disregarded, such conduct.⁹⁸ The defense is broadly conceived to include most instances of vicarious or imputed liability of employers.

The two good-faith defenses, also defined in other sections of the statute as "Good Samaritan" actions,⁹⁹ contemplate "reasonable, effective, and appropriate actions" taken in good faith under the circumstances, in order to restrict or prevent access by minors.¹⁰⁰ The word "effective" is qualified as not requiring "an absolute 100% restriction of access."¹⁰¹ The other defense consists in the implemented restriction of access "by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number."¹⁰² The Federal Communications Commission (FCC) "may describe measures which are reasonable, effective, and appropriate to restrict access," but is not empowered to enforce, "approve, sanction, or permit, the use of such measures."¹⁰³ The use of the measures described by the FCC as "reasonable, effective, and appropriate," however, "shall be admitted as evidence of good faith efforts."¹⁰⁴

Finally, the Act preempts any state or local regulations imposing liability in a way inconsistent with the treatment provided under the Act.¹⁰⁵ State and local governments, however, can enact complementary regulations limited to intrastate services, and not inconsistent with the provisions governing interstate services.¹⁰⁶ The limitation on state and local governments "is intended to establish a uniform national standard of content regulation for a national, and indeed a global, medium."¹⁰⁷

Immediately after the Act was signed into law, the American Civil Liberties Union and nineteen other plaintiffs—all providers and users of on-line communications—requested a federal judge in Philadelphia to issue a temporary restraining order (TRO) enjoining the government from enforcing against them the provisions contained under 47 U.S.C. §§ 223(a)(1)(B) and 223(d).¹⁰⁸ The plaintiffs claimed that they would be irreparably harmed as a result of the vagueness of the terms "indecent" and "patently offensive" contained in the Act.¹⁰⁹ The vagueness of such terms, which define criminal violations under the Act, would unavoidably expose the plaintiffs to the risk of criminal prosecution, provoking a chilling effect on the exchange of communications on important issues.¹¹⁰ The judge, while recognizing that "Congress has a compelling interest in protecting the physical and psychological well-being of minors," and that Congress had not failed to narrowly tailor the CDA,¹¹¹ issued the requested TRO, holding that the plaintiffs had raised a substantial question whether "the use of the undefined term, 'indecent' " in 47 U.S.C. § 223(a)(1)(B)(ii) is "unconstitutionally vague."¹¹² The ruling rejects the government's argument that the term "indecent" contained in section 223(a)(1)(B)(ii) has the same meaning as the clause "patently offensive" contained in section 223(d)(1)(B).¹¹³

A few days after the publication of the order, a large group of technology companies, trade associations, non-profit organizations and libraries filed another lawsuit in the same court.¹¹⁴ The suit will probably be argued on the breadth and vagueness of the statute, as well as on its redundancy, because there are less drastic means of protecting children from obscene material. The plaintiffs also intend to explain how the Internet differs in nature from other media.¹¹⁵

One of the many concerns raised by the new Act is that banning indecent or patently offensive communications from a pervasive means of communications such as the Internet may realistically amount to an overall censorship. The terms "indecent" and "patently offensive" can be qualified in very different manners in different parts of the country. In general, the test to determine whether particular material is obscene refers to *local* community standards,¹¹⁶ rather than to a national standard. Thus, the Act creates the risk that the qualification of on-line communications as "indecent" or "patently offensive" will mirror the qualification that those terms receive in the most conservative and strict communities. The result would be that a considerable amount of valuable discussion on politics, sciences and arts would be measured on the basis of the most severe standards, and would ultimately be driven from the Internet.

D. Traditional Mail v. E-Mail

The Communications Decency Act of 1996 introduces relevant, though controversial, measures to enhance the protection of on-line privacy. Even absent this Act, however, there are situations, probably even more inclusive than those contemplated in the Act, where current rules of liability may apply to a sysop. Indeed, a likely analogy can be suggested between traditional mail, also referred to as "snail-mail" by Internet users, and e-mail. Sysops, like the Postal Service, may be required to act to protect their customers in some situations where the mail is used for harmful purposes.

Under Part IV of the Postal Reorganization Act of 1970, Chapter 30-NonMailable Matter,¹¹⁷ a person may require that a mailer refrain from further mailings and remove his name from its mailing lists. Under this section, entitled "Prohibition of pandering advertisements,"¹¹⁸ a person has the right to insulate himself from advertisements that "offer for sale matter which the addressee in his sole discretion believes to be erotically arousing or sexually provocative."¹¹⁹ The Postal Service, upon receipt of notice from the addressee, must issue an order "directing the sender and his agents or assigns to refrain from further mailings to the named addressees."¹²⁰ Additionally, the Postal Service is required to order the affected sender to delete the name of the designated addressee from all mailing lists owned or controlled by the sender, and to prohibit "the sale, rental, exchange, or other transactions involving mailing lists bearing the names of the designated addressees."¹²¹

In *Rowan v. United States Post Office Department*,¹²² the Supreme Court upheld the statute as constitutional.¹²³ The Court noted that Congress intended the law to protect citizens' privacy, and further noted that possible constitutional questions which might arise from vesting a governmental official with such power were precluded by the right to a full hearing offered to the sender.¹²⁴ The Court then held that not only pandering advertisements but *all* further mailings by the sender to the addressee are prohibited, after an order or direction by the Postmaster General.¹²⁵

It would be anomalous to read the statute to affect only similar material or advertisements and yet require the Postmaster General to order the sender to remove the addressee's name from *all mailing lists* in his actual or constructive possession. The section was intended to *allow the addressee complete and unfettered discretion* in electing whether or not he desired to receive further material from a particular sender [T]he right of every person "to be let alone" must be placed in the scales with the right of others to communicate. In today's complex society we are inescapably captive audiences for many purposes, but a sufficient measure of individual autonomy must survive to permit every householder to exercise control over unwanted mail [A] mailer's right to communicate must stop at the mailbox of an unreceptive addressee To hold less would tend to license a form of trespass and would make hardly more sense than to say that a radio or television viewer may not twist the dial to cut off an offensive or boring communication and thus bar its entering his home.¹²⁶

This reasoning easily can be extended to include the right to require a sysop to block unwanted communications in the name of the right "to be let alone."¹²⁷

The basic freedom to communicate and distribute information, which the Court set forth in *Martin v. City of Struthers, Ohio*,¹²⁸ does not conflict with an individual's right "to be let alone" and exercise control over unwanted communications. In *Martin*, the conviction of a Jehovah's Witness for knocking on doors to distribute handbills in violation of a city ordinance was vacated by the Supreme Court, which held the ordinance invalid because it was in conflict with the freedom of speech and press.¹²⁹ However, while stating that the "[f]reedom to distribute information to every citizen wherever he desires to receive it is so clearly vital to the preservation of a free society that . . . it must be fully preserved,"¹³⁰ the same Court recognized that time and manner of distribution may be regulated, and acknowledged a limitation in terms of leaving "with the homeowner himself" the power to decide "whether distributors of literature may lawfully call at a home."¹³¹ Moreover, it clarified that what makes a person entering the property of another a trespasser is the existence of an "explicit command from the owners to stay away."¹³²

Thus, a network user's affirmative request that the sysop block further communication from a certain sender may well amount to an explicit command to protect the domain of his private life. The principle underlying the Postal Service statute, and the broader protections of individual privacy, suggest that e-mail and network communications should be protected as well, even where the protection of the user's privacy is not regulated in the subscription contract. The activity statutorily required from the Postal Service could be similarly required from a sysop.¹³³ Upon a simple notice, the sysop should stop any message coming from a certain sender (identified or anonymous) from reaching the personal account. In the case of electronic mail, the sysop might be required to set up a program that automatically rejects mail coming from certain senders. A program could also be used to search through the text of an incoming message and reject any message containing certain terms which the receiver would not want to receive. Failure of the sysop to do so could result in liability for omission of required activity.

E. Conclusion

The nature of the electronic means increases the magnitude of the privacy issues considered. The violation of privacy also extends to cases where there is no entry at all. The Electronic Communications Privacy Act of 1986¹³⁴ (ECPA) reflects dramatic changes in new computer and telecommunications technologies. Sysops might be liable if they negligently make possible the intrusion into the private affairs of a user. The ECPA allows sysops to record the fact that an electronic communication was initiated or completed in specific cases, in order to insure protection from fraudulent, unlawful or abusive use of the service. They may therefore install adequate technological safeguards for the privacy of the material loaded onto their systems. The adoption of reasonable, effective and appropriate actions to prevent illicit use of the system may eventually amount to a valid defense in favor of the sysop, similar to the defenses afforded by the Communications Decency Act.

Thus the general common law, constitutional law and a number of statutes will bear on the liability of sysops for violations of their customers' privacy. The basic principle of the protection of privacy suggests that this liability may be somewhat high. And indeed, in a number of situations the sysop may be held liable for failure to protect customers or otherwise bear an affirmative duty to take action to protect customers' privacy. But the most recent statutes include some protections for sysops, showing that Congress recognizes that overuse of vicarious liability will deter useful Internet growth. These two principles-protection of the customer and promotion of the Internet-conflict as well in our next discussion, liability for defamation and related torts. This area also raises significant First Amendment concerns, this time not for the rights of the violated, but those of the alleged violators.

IV. Flaming¹³⁵

Public discourse raises the danger of the tort of defamation, and this is as true on the Internet as in any other public setting. Defamation is the denigration of an individual's standing in the community, impinging on his reputation and good name.¹³⁶ Defamation can easily be committed by users through e-mail, newsgroups, chat or other electronic services. On-line communications may invade an individual's right to privacy as well. The right to privacy not only protects an individual's seclusion, solitude or private affairs, but also forbids the public disclosure of embarrassing private facts, publicity that places someone in a false light in the public eye and the appropriation of someone's name or likeness.¹³⁷ There is no doubt, however, that an electronic communication belongs to the category of speech, and freedom of speech is protected by the First Amendment. How can we reconcile the rights of privacy and freedom from defamation with freedom of speech?

Sysops sometimes do not allow users to post messages that, in their opinion, approach the limits of acceptable speech. In addition, many small bulletin boards may limit access to those individuals whom the operator knows personally. Since the First Amendment protects citizens only against the actions of government, a sysop can censor users without violating the First Amendment.¹³⁸ Therefore, restrictions imposed by sysops do not constitute a limitation of speech in the constitutional sense. However, governmental imposition of liability on either the speaker or the sysop raises such constitutional questions. Does uncertainty about the applicable standard of liability, or the imposition of unnecessarily high liability, have a damaging effect on free speech, by giving sysops an incentive to limit access or censor communications?

General principles of constitutional protection of speech, as well as the first few decisions on these issues, may help us predict the situations in which a sysop may be held liable for the on-line torts of a user. This part will discuss these cases, and suggest how the principles of constitutional protection should be applied to the new realm of cyberspace to reconcile the protection of the innocent with the vital rights of freedom of speech.

A. Defamation

A defamation suit has profound First Amendment implications. By definition, libel involves a publication or communication of the defendant's views to some third person.¹³⁹ Nevertheless, defamation is primarily a state cause of action. The consequence is that

adjudication of such claims requires inquiries into both federal and state law.¹⁴⁰ Defamation is also closely related to invasion of privacy, but while privacy actions involve emotional and mental suffering, defamation actions involve injury to reputation.¹⁴¹

The potential for on-line defamation is great. A defaming message can be transmitted freely across borders and into millions of homes with little effort. Damaging allegations made during a chat session or through distribution of text files can be extremely harmful.¹⁴² Defamation law protects a person's reputation from harm caused by false and damaging statements.¹⁴³ As with written media, defamatory remarks in cyberspace are mostly classified as libel. The plaintiff must show that the language has been published to an audience composed of people other than the plaintiff.¹⁴⁴ Thus, on the Internet, if copies of e-mail are sent to other persons, if the message is publicly distributed in some other way, or if the message is posted to a bulletin board or in a newsgroup, the requisite publication has occurred.¹⁴⁵

A network user may certainly sue the alleged defamer for damages. But may he also sue the system operator who made the defamation possible?

1. *The New York Times Framework*

*New York Times v. Sullivan*¹⁴⁶ established the basic framework for analyzing the constitutionality of a defamation claim. A police commissioner brought a civil libel action not only against four black persons but also against the New York Times Company for an advertisement published in the *New York Times*. Writing for the Court, Justice Brennan projected the First Amendment onto state libel law by holding that the states may not impose strict liability upon media defendants in defamation cases brought by public officials.¹⁴⁷ *Sullivan* established an "actual malice" standard-liability requires "knowledge that [the statement] was false" or "reckless disregard of whether it was false or not."¹⁴⁸

Consequently, different degrees of fault are required depending on who the plaintiff is. Actual malice is not required for liability to non-public figures, people who have not put themselves into the public eye and are not involved in issues of public concern. This is because private citizens often do not have the means to access mass media to rebut or disprove the damaging comments. The Supreme Court in *Sullivan* also made it clear that the First Amendment embodies two principles: that speakers should be free from government censorship and that "debate on public issues should be uninhibited, robust, and wide-open."¹⁴⁹ Since public figures have a diminished expectation of privacy,¹⁵⁰ and the public has a greater need to know information about such figures than about purely private people,¹⁵¹ the application of different standards depending on the plaintiff's status, helps reconcile the right to privacy and the constitutional guarantee of free speech and a free press.¹⁵²

In *Gertz v. Robert Welch, Inc.*,¹⁵³ the plaintiff, an attorney, was accused in print of organizing a "communist frameup" of a policeman. He sued for defamation. The Supreme Court appeared to narrow the *Sullivan* rule, allowing states to impose an ordinary negligence standard "for a publisher or broadcaster of defamatory falsehood injurious to a *private* individual."¹⁵⁴ However, the Court held that damages are normally limited to compensation for actual injury, and that only when actual malice has been proven can the private individual plaintiff also recover punitive and presumed damages.¹⁵⁵ In an action for libel, in fact, no proof of actual injury is required for recovery-injury is presumed from the fact of publication.¹⁵⁶ This gives juries uncontrolled discretion to award judgments unrelated to any actual injury, which could be used to punish unpopular opinions and inhibit the vigorous exercise of First Amendment freedoms.¹⁵⁷ Limiting awards to actual damages in the absence of actual malice protects such unpopular speakers from unnecessary liability-a clear and interesting statement of public policy about the priority of protection of free speech over uncontrolled judicial discretion.

Gertz also explains why it makes sense to give public figures less protection than private individuals. Justice Powell wrote for the Court that it had

no difficulty in distinguishing among defamation plaintiffs. The first remedy of any victim of defamation is self-help-using available opportunities to contradict the lie or correct the error and thereby to minimize its adverse impact on reputation. Public officials and public figures usually enjoy significantly greater access to the channels of effective communication and hence have a more realistic opportunity to counteract false statements than private individuals normally enjoy. Private individuals are therefore more vulnerable to injury, and the state interest in protecting them is correspondingly greater.¹⁵⁸

"[P]rivate individuals are not only more vulnerable to injury than public officials and public figures, they are also more deserving of recovery."¹⁵⁹ Thus, the ordinary negligence standard applies to them.

The Supreme Court has refined the *Gertz* rule in more recent cases. Where the defamatory statement does not involve matters of public concern, the Court has underscored the right of private individuals to presumed and punitive damages. In *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*,¹⁶⁰ a credit-reporting agency falsely indicated that a construction contractor had filed a petition for bankruptcy. The Court considered that "the role of the Constitution in regulating state libel law is far more limited when the concerns that activated *New York Times* and *Gertz* are absent."¹⁶¹ The majority opinion by Justice Powell held that when the defamation does not involve matters of public concern, "the state interest adequately supports awards of presumed and punitive damages—even absent a showing of 'actual malice.'"¹⁶²

On the other hand, in suits by public figures, the Court has reaffirmed the actual malice requirement. In *Hustler Magazine v. Falwell*,¹⁶³ the Court examined a suit against a publisher for intentional infliction of emotional distress. A parody portrayed the plaintiff, a minister and commentator on public affairs, as having committed incest with his mother in an outhouse.¹⁶⁴ The opinion, written by Chief Justice Rehnquist, held that a public figure cannot recover damages for emotional distress without satisfying the *New York Times* standard, and that the plaintiff had not proven that the parody constituted a false statement of fact.¹⁶⁵ Since the seemingly malicious motive was not accompanied by falsity as to facts, the "actual malice" requirement was not met.

How do these standards apply in cyberspace? In cyberspace, everyone has a similar ability to communicate with large numbers of people. In some situations, such as a bulletin board discussion, users voluntarily inject themselves into public controversies. Is this sufficient to make the "actual malice" standard applicable to them? When a private person is involved in an issue of public concern, the higher standard may be applicable,¹⁶⁶ limiting liability for defamation. But is participation in a public discussion on the Internet equivalent to participation in a matter of public concern?¹⁶⁷

For individuals who voluntarily seek public attention and therefore become public persons subject to fair comment and criticism, the answer is yes. A different conclusion might result in the case of individuals who do not exploit their personalities to attain fame or to become public figures. However, Internet users who fall between these two categories, but who become public figures by the force of circumstances beyond their control, present an awkward problem.¹⁶⁸ In this age of "media hype," the number of public figures cannot be limited to predetermined categories,¹⁶⁹ and each situation must be considered individually.

Since defamation victims on the Net have the same ability to communicate with large audiences as their alleged defamers, and thus enjoy the opportunity to correct an error or contradict a lie, they can minimize the impact on their reputations. This supports the application of the public figure standard in cases of alleged defamation over the Net. Indeed, an ordinary negligence standard (like the one in *Gertz*) imposes an intolerable burden on system operators. Print and broadcast media exercise full editorial control over the published material. They employ staffs to research, edit and proofread material that is published or broadcast. Most system operators, instead, do not engage in such extensive prescreening of submitted material, and probably lack the necessary resources to do so. Should the requisite editorial control become a cost of doing business, or should a different standard of liability apply to unedited Net communications? A significant risk of liability would force many operators to shut down these boards, leaving the industry in the hands of the large and powerful commercial services.¹⁷⁰ This would significantly impair the "uninhibited, robust, and wide-open" debate so valued under the First Amendment.

The interaction of these standards with the new setting of cyberspace has already resulted in a few court decisions which supply us with some hints as to the outcome of this new field of law. Not surprisingly, the outcomes seem somewhat inconsistent. Yet an analysis of the cases reveals the beginnings of a framework for predicting when a sysop will be held liable for the defamation of a user.

B. *Cubby v. CompuServe*

One of the pioneer cases that specifically addressed the liability of a computer network operator for posting material submitted by a user was *Cubby, Inc. v. CompuServe, Inc.*¹⁷¹ This was an action brought against a computer service company, CompuServe, for an alleged libel published on its system.¹⁷² The District Court granted the company's motion for summary judgment, holding that the company was a mere "distributor" of information, and therefore could not be held liable absent a showing that it knew or had reason to know of defamation.¹⁷³

A detailed explanation of the facts is necessary to understand the extent and the boundaries of the decision. CompuServe runs special interest "fora," each one including electronic bulletin boards, interactive on-line conferences and topical databases.¹⁷⁴ One forum, regulated and controlled by Cameron Communications, Inc. (CCI), an independent contractor, focused on the journalism industry. CCI's control was exercised "in accordance with editorial and technical standards established by CompuServe."¹⁷⁵ Don Fitzpatrick Associates of San Francisco (DFA) was the publisher and on-line provider of Rumorville USA, a daily newsletter providing reports about journalism and journalists. It was alleged that "CompuServe had no employment, contractual, or other direct relationship with

either DFA or Fitzpatrick."¹⁷⁶ It was also alleged that "CompuServe had no opportunity to review Rumorville's contents before DFA upload[ed] it into CompuServe's computer banks, from which it was immediately available to approved . . . subscribers."¹⁷⁷ When Rumorville published allegedly false and defamatory statements relating to Cubby, Inc., the latter immediately brought a lawsuit under New York libel law. There was no dispute on the defamatory contents of the statements. Rather, CompuServe argued that "it acted as a distributor, and not as a publisher, of the statements, and [could] not be held liable for the statements because it did not know and had no reason to know of the statements."¹⁷⁸

The court noted that although "one who repeats or republishes defamatory matter is subject to liability as if he had originally published it,"¹⁷⁹ news vendors, bookstores and libraries "are not liable [in New York courts] if they neither know nor have reason to know of the defamation."¹⁸⁰ District Judge Leisure also pointed out that "the requirement that a distributor must have knowledge of the contents of a publication" before incurring liability "is deeply rooted in the First Amendment."¹⁸¹ CompuServe carried the publication as part of a forum that was managed by an unrelated company, CCI. Moreover, DFA could upload the text of Rumorville into CompuServe's library and make it available to its users instantaneously.¹⁸² Because CompuServe had no more editorial control over the publication's contents than does a library, bookstore or newsstand, and because "[a] computerized database is the functional equivalent of a more traditional news vendor," a standard of liability higher than that imposed on those categories "would impose an undue burden on the free flow of information."¹⁸³

Cubby v. CompuServe does not resolve what happens when the sysop is aware of the contents and allows distribution anyway. It might be inferred from the decision that in such a case the sysop would be as liable as the primary publisher. However, such a rule would give the sysop a somewhat perverse incentive not to know the contents of materials offered on its bulletin board. This may lower the quality or the standard of its service.

Another unresolved question is whether a sysop is liable for defamation occurring on a message base or newsgroup. Unlike in *CompuServe* (where DFA was the publisher of the daily newsletter Rumorville), the question becomes whether the libeler who uploads the file in the newsgroup or the sysop who implements the publication should be considered the "publisher."

Finally, *CompuServe* was decided upon a special contractual agreement in which CompuServe waived any responsibility for the content of the newsletter, Rumorville USA. In fact, CCI was in control of the contents of the published material.¹⁸⁴ Without this type of relationship, the outcome would certainly have been different.

In all likelihood, another judge might decide an analogous case in a different fashion. Indeed, even though *CompuServe* was not tried in court and was decided upon a motion for summary judgment, there are undisputed facts that qualify the decision as questionable, at the least. The judge found that CompuServe had "simply contracted with CCI for CCI to manage the Journalism Forum,"¹⁸⁵ and that it had thereby delegated control over the assembly of the contents of the forum.¹⁸⁶ At the same time, though, he recognized that CompuServe had the "right under the contract to remove text from its system for noncompliance with its standards."¹⁸⁷ Other contractual provisions required CompuServe to furnish the necessary training and to indemnify CCI for claims resulting from information appearing in the forum. Nevertheless, this level of control was deemed insufficient to rise to the level of an agency relationship,¹⁸⁸ and Cubby's contention that CompuServe be held vicariously liable was rejected. Regardless of the potential liability of an independent contractor like CCI,¹⁸⁹ in a similar factual case a different outcome could be expected, based on the same legal assumptions, but on a more accurate recognition of facts and relationships involved.

C. Stratton Oakmont, Inc. v. Prodigy Services Co.

The recent case of a multimillion dollar suit against Prodigy deserves some attention. The decision for the first time recognized the system operator's liability as a publisher. In *Stratton Oakmont, Inc. v. Prodigy Services Co.*,¹⁹⁰ the court granted plaintiffs' motion for partial summary judgment against defendant Prodigy and determined, as a matter of law, that Prodigy was a "publisher" of statements concerning plaintiffs on its computer bulletin board for the purposes of plaintiffs' libel claims, and that the board leader¹⁹¹ of Prodigy's computer bulletin board acted as Prodigy's agent.

The facts are simple. An unidentified user of Prodigy's "Money Talk" computer bulletin board¹⁹² accused plaintiff Stratton Oakmont, Inc., a securities investment banking firm, of criminal and fraudulent conduct. Stratton Oakmont sued Prodigy, as the owner and operator of the computer network on which the statements appeared. The evidence on which the plaintiff relied included Prodigy's guidelines, in which users are requested to refrain from posting notes that are "insulting" and are advised that harassing notes will be removed when brought to Prodigy's attention.¹⁹³ The plaintiff also pointed to Prodigy's use of software which "automatically prescreens all bulletin board postings for offensive language."¹⁹⁴

The court characterized the critical inquiry as whether the evidence "establishe[d] a prima facie case that Prodigy exercised sufficient editorial control over its computer bulletin boards to render it a publisher."¹⁹⁵ The court distinguished *CompuServe* in two ways. "First, Prodigy held itself out to the public and its members as controlling the content of its computer bulletin boards," whereas CompuServe had no similar control.¹⁹⁶ "Second, Prodigy implemented this control through its automatic software screening program, and the Guidelines which Board Leaders [were] required to enforce."¹⁹⁷ "By actively utilizing technology and manpower to delete notes from its computer bulletin boards," Prodigy screened the content of messages posted on its boards, and this constituted editorial control. Therefore, Prodigy was a publisher rather than a distributor.¹⁹⁸

A distributor is considered a passive conduit and cannot be found liable in the absence of fault.¹⁹⁹ A publisher such as a newspaper, on the other hand, "is more than a passive receptacle or conduit for news, comment and advertising."²⁰⁰ A publisher exercises editorial control by choosing the material to be published, and this editorial control increases the publisher's liability.²⁰¹ Here, the creation of an editorial staff which had the ability to monitor incoming transmissions altered the *CompuServe* scenario.

The judge dismissed the possibility that the decision would compel all computer networks to abdicate control of their bulletin boards, refusing to presume that the market will compensate a network for its increased control and the resulting increased exposure.²⁰²

On the second issue presented, whether the board leader was Prodigy's agent, the judge based his decision on the analysis of the "Bulletin Board Leader Agreement."²⁰³ The Agreement contained language excluding any representation and assumption of liabilities by Prodigy for any acts or omissions of the board leader, and excluded any employment or agency relationship as well.²⁰⁴ However, it did require Prodigy's prior approval of all promotional efforts.²⁰⁵ By looking into the substance of the relationship, the judge held that since Prodigy retained a sufficient degree of direction and control over the board leader, a principal-agent relationship existed, and, in addition, that "whether one is an independent contractor is not determinative of whether one is an agent."²⁰⁶

After entry of the partial summary judgment, the parties settled their case. Prodigy then moved to vacate, but Judge Ain refused to overturn the ruling.²⁰⁷

Prodigy is the first ruling to hold that an on-line service is not merely a passive transmitter of information, but essentially a publisher, responsible for the content of material posted on its electronic bulletin boards. The decision seems to fill in the gaps left open in *CompuServe*, reaching exactly the opposite conclusion. However, the approach of analyzing the sysop's control over the information available on the system in order to estimate its liability was common to both decisions. As a further step, any future analysis should inquire into the different aspects that the sysop's activity may assume, and the different liabilities that may attach to it.

D. Religious Technology Center v. Netcom On-line Communication Services, Inc.

Although copyright issues are beyond the scope of this article, on-line copyright infringement is another area in which sysops may be held liable. A recent case, *Religious Technology Center v. Netcom On-line Communication Services, Inc.*,²⁰⁸ warrants a brief detour. The issue in *Netcom* was whether an Internet service provider and operator of a BBS should be liable for copyright infringement committed by a subscriber of the BBS who used the ISP to access it.

Plaintiffs owned copyrights in the works of the founder of the Church of Scientology. One of the defendants, Mr. Erlich, was a critic of the Church. He discussed and criticized the Church on an on-line forum on a BBS run by defendant Klemesrud, and he was given access to the Internet by defendant Netcom On-line Communications, Inc.²⁰⁹ When the plaintiffs asked Klemesrud to stop Erlich's postings, Klemesrud asked them to prove that they owned the copyright. Then the plaintiffs contacted Netcom. Netcom, however, refused to interrupt the Internet connection, contending that it would be impossible to pre-screen all the postings.²¹⁰

On the issue of Netcom's liability for direct copyright infringement, the court granted Netcom's motion for summary judgment, considering that "it does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringement is nothing more than setting up and operating a system that is necessary for the functioning of the Internet."²¹¹ The court noted that Netcom did not create, control or monitor the content of the information²¹² and did not voluntarily create copies of the protected works.²¹³ Nevertheless, the court refused to hold Netcom to be a common carrier,²¹⁴ because Netcom was not a mere passive means of information and did more than just "provide the wire and conduits."²¹⁵

On the issue of Netcom's liability for contributory infringement, though, the court found "a question of fact as to whether Netcom knew or should have known that Erlich had infringed plaintiff's copyrights following receipt of plaintiff's letter,"²¹⁶ and, therefore, "as to whether Netcom knew of any infringement by Erlich before it was too late to do anything about it."²¹⁷ The court concluded that

Netcom's failure to cancel the message and stop the worldwide distribution of the copies could constitute "substantial participation in [the infringement]."218

Finally, on the issue of Netcom's vicarious liability, the court granted Netcom's motion for summary judgment.²¹⁹ Even though the judge found that Netcom could have possibly exercised control over the activities of Erlich, its subscriber, nevertheless there was no evidence of any direct financial benefit that Netcom could possibly receive from the infringing activities.²²⁰

Netcom's knowledge seems to be the focus of the court's attention. If Netcom had knowledge of the alleged infringement at the time the protected works were posted on its network, then Netcom could be contributorily liable because it took no action to investigate. Also, the ruling is important because the judge rejected the claim of Netcom's and Klamesrud's direct infringement.²²¹ Direct copyright infringement is based on a strict liability standard and does not require knowledge or intent by the infringer. Such a standard would have imposed on sysops the heavy burden to screen all information in transit on their systems. The judge, instead, required the plaintiffs to establish at trial Netcom's and Klamesrud's contributory infringement, which requires knowledge of the infringement and substantial participation in it.²²²

E. Analogies for Sysop's Liability

CompuServe compared the position of the sysop to that of a library, bookstore or newsstand. *Prodigy*, on the other hand, held the sysop to be a publisher with the same responsibilities as a newspaper. The differences in *CompuServe* and *Prodigy* can be explained by the different analogies they use to determine sysop liability.²²³ It is important to determine which distinguishing characteristics of sysops warrant special consideration in selecting the appropriate levels of legal rights and obligations.²²⁴ Crafting rules narrowly tailored to both the specific factual situations and the functional capabilities of sysops, rather than adopting static global rules, will allow this sensitivity to inform individual decisions.²²⁵

1. The Sysop as a Common Carrier

It is generally argued that bulletin boards, networks or on-line services are common carriers, and that they should be protected as such.²²⁶ The transmission of data on a computer information system works in a way similar to the activity of a common carrier. But a computer information system that can act at times like a common carrier, and at times like a publisher, need not be classified according to only one communications analogy.

Common carriers are services like telephone, telegraph and satellite communications. They must "furnish service upon reasonable request" and cannot "make any unjust or unreasonable discrimination."²²⁷ Liability for defamation adheres only when the carrier knows that the material is defamatory, provided that the sender of the defamatory message is not privileged.²²⁸ This knowledge standard, coupled with the privilege exception, is designed to secure efficiency, fairness and privacy.²²⁹ The Electronic Communications Act of 1986²³⁰ incorporates a similar knowledge standard and includes sysops as well as common carriers within its scope.²³¹ The statute generally prohibits the *intentional* interception and use of intercepted e-mail and network communications,²³² and directs that "a person or entity providing an electronic communication service to the public," a definition in which the system operator is certainly included, cannot *intentionally* divulge the contents of any communication.²³³ Thus this law supports the common carrier analogy.

However, the common carrier argument does not seem entirely applicable to most sysops. Common carriers are characterized by the unlimited access they must offer to anyone who asks for it, and by the duty to transmit upon request.²³⁴ But sysops are free to limit access to their systems. If sysops were obliged to transmit automatically and instantaneously all the information they receive, they could not exercise any editorial control over the contents of their system. Given the enforcement of strict policies pursued by many sysops, this requirement would hardly be accepted.²³⁵

2. Sysop as Press: Braun v. Soldier of Fortune

The common carrier analogy does not apply to public message areas. Messages posted in these areas are accessible to a much wider audience than messages transmitted by common carriers, which are received only by the specified addressee. Moreover, computer networks have not yet become essential means of communication in the same way as telephones and, therefore, do not at this time require regulation of their activity analogous to that applied to common carriers. On the other hand, sysops have potential editorial control over the content of their system. Can the sysop, as a consequence of such editorial control, be held liable to the same extent as the press in these cases? What would the consequent liability be?

In an action against a magazine publisher for injuries sustained from fireworks purchased by plaintiffs through a paid advertisement in the magazine, the Superior Court of New Jersey, Appellate Division, held that a publisher was not liable where he did not guarantee, warrant or endorse the product, although the magazine was allegedly a pseudoscientific publication.²³⁶ Subsequent decisions have confirmed that readers of publications of unintentionally fraudulent or erroneous information are not entitled to damages against the publisher.²³⁷

A key case is *Braun v. Soldier of Fortune Magazine, Inc.*²³⁸ A man who had decided to murder his business partner contacted a mercenary who advertised in the magazine. He then shot the victim with the mercenary's help. The sons of the murder victim brought an action for wrongful death against the magazine and its parent company, alleging that the defendants negligently published an advertisement that created an unreasonable risk of criminal activity.²³⁹ The jury awarded compensatory and punitive damages, and the magazine appealed. Applying Georgia law, the Court of Appeals held that publishers owe "a duty to the public when they publish an advertisement if 'the ad in question contain[s] a clearly identifiable unreasonable risk.'"²⁴⁰

The court then resolved the implicated First Amendment interest in commercial speech by noting that the First Amendment does not protect speech related to an illegal activity.²⁴¹ Citing past Supreme Court decisions, the court held that the negligence standard permitted by the First Amendment in such cases is a "modified" one²⁴² imposing "no legal duty to investigate the ads" on the publisher.²⁴³ Only an ad that would "on its face" alert a reasonably prudent publisher could generate his liability.²⁴⁴ In order to determine whether the risk was "unreasonable," the court applied a risk-utility balancing test, in which "[the] liability depends upon 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."²⁴⁵ It then concluded that the district court properly instructed the jury that the magazine could be held liable "if the advertisement on its face would have alerted a reasonably prudent publisher to the clearly unreasonable risk of harm to the public that the advertisement posed."²⁴⁶ This reasonable foreseeability of the consequences also gave the jury ample grounds for finding that Soldier of Fortune's publication of the ad was the proximate cause of the death and that the chain of causation was not broken.²⁴⁷

The framework proposed in *Braun* could be extended to determine the potential liability of the sysop. This framework would require the plaintiff to establish that a certain activity that would have alerted a reasonably prudent sysop took place on the system. The plaintiff would have the burden of proving the probability of harm and the injury likely to result, and the burden of persuasion on the issue of the unreasonableness of the risk taken by the sysop.²⁴⁸ The sysop, on the other hand, could avoid liability by proving that it adopted adequate precautions or that the burden of doing so would have outweighed the harm. Therefore, different outcomes may result on a case-by-case basis.

This paradigm ignores the fact that, while big system operators like Prodigy employ a staff to monitor material submitted for posting, most other commercial networks do not.²⁴⁹ Moreover, even where a sysop has implemented the same editorial control that a print publisher has, the volume of the material may effectively prohibit actual editorial control over what is being transmitted through the computer system. In fact, operators of large systems claim that the job of monitoring every communication on their system is a prohibitively large task. In some situations, the only defense available to the sysop might be the risk-utility balancing test.²⁵⁰

3. Sysop as Republisher/Disseminator/Distributor

Another useful analogy is to compare sysops to secondary distributors such as booksellers and libraries. Like common carriers and the press, such secondary distributors may be held liable only if they knowingly possess defamatory or obscene material.²⁵¹ A republisher or disseminator, who circulates, sells or otherwise deals in the physical embodiment of the published material, is similarly protected.²⁵² Computer system operators fit into the republisher paradigm because they make files available just as a bookseller or library makes texts available.

In *Smith v. California*,²⁵³ the Court struck down an ordinance imposing criminal liability solely for possession of obscene material. The Court held that such liability cannot be imposed on a secondary distributor without provoking self-censorship. In fact, "if the bookseller is criminally liable [even] without knowledge of the contents . . . he will tend to restrict the books he sells to those he has inspected."²⁵⁴ The consequence would be "a restriction" upon the distribution of constitutionally protected as well as obscene literature Every bookseller would be placed under an obligation to make himself aware of the contents of every book in his shop."²⁵⁵

The *Smith* case was the first to break from common law tradition and establish immunity from liability for distributors.²⁵⁶ However, *Smith* did not determine the degree of liability appropriate for a bookseller, although it did find that strict liability was too restrictive.²⁵⁷ In the case of sysops, although it is technologically possible to require computer bulletin board operators to prescreen

messages submitted for posting, imposing such an obligation on them could be equivalent to censoring them.²⁵⁸ The flow of communication would dry up substantially as small board operators who could not screen large numbers of messages would be forced either to limit postings or shut down. Needless to say, the attraction of communication over computer bulletin boards lies in the instant interaction they make possible. Accordingly, in order to foster the optimum freedom of expression on computer networks, sysop's liability should apply only when the sysop knows that an obscene, illegal or defamatory message is posted on the system, or when the sysop does not remove such a message once it has been made aware of its existence.

It follows that if the sysop (as a secondary publisher) does not know nor has reason to know of the content of the publications it offers to the public, it should not be liable.²⁵⁹ Any different conclusion would put too heavy a burden on the sysop (like the librarian) to review everything it distributes to the public, a burden that, if enforced, would hamper the ability to supply a large amount of diverse information in a timely fashion.²⁶⁰

4. Sysop as Bulletin Board

Another potential source of guidance as to sysop liability is the line of cases dealing with bulletin boards and other public places where messages and notices are posted. The foundational case in this line is *Fogg v. Boston & L. R. Co.*,²⁶¹ an old case in which a newspaper article defaming a ticket broker was posted in the defendant's railway office on a bulletin board maintained for public view.²⁶² The court decided that a jury could have concluded that the defendant, through its agents, had knowledge of what was posted in its office.²⁶³ Also, the article was placed in the station, in an area related to the business that the defendant conducted therein,²⁶⁴ and had not been removed in a timely manner. Thus, even if the company was not responsible for its posting in the first place, the failure to remove the article promptly could amount to constructive authorship, endorsement or ratification.²⁶⁵

The rule stated in *Fogg* has been upheld in more recent cases. *Hellar v. Bianco*²⁶⁶ was an action against the proprietors of a public tavern for damages for a libelous publication written on the wall of the men's restroom, concerning the chastity of the plaintiff.²⁶⁷ The court held that

[p]ersons who invite the public to their premises owe a duty to others not to knowingly permit their walls to be occupied with defamatory matter . . . [B]y knowingly permitting such matter to remain after reasonable opportunity to remove the same the owner of the wall or his lessee is guilty of republication of the libel.²⁶⁸

Even though the proprietor was originally unaware of the defamation, the plaintiff had complained to the bartender, asking him to remove the inscription from the wall. Reasoning from the bartender's knowledge, the court held that "the knowledge of an agent, while acting in the scope of his authority, is imputed to the principal."²⁶⁹

An apparently different conclusion was reached in a more recent case, *Scott v. Hull*.²⁷⁰ Graffiti defaming the plaintiff was inscribed on the side of a building. The plaintiff gave notice of its existence and demanded removal, but neither the owner of the building nor the agent took any action.²⁷¹ Recognizing the rule applied in *Fogg* and *Hellar*, but claiming to distinguish these cases, the court observed that "liability to respond in damages for the publication of a libel must be predicated on a positive act," and that "[n]onfeasance . . . is not a predicate for liability."²⁷² Therefore, it concluded that

where liability is found to exist it is predicated upon actual publication by the defendant or on the defendant's ratification of a publication by another, the ratification in *Hellar v. Bianco* and *Fogg v. Boston & L. R. Corp.* consisting of at least the positive acts of the defendants in continuing to invite the public into their premises where the defamatory matter was on view after the defendants had knowledge of the existence of same.²⁷³

In the facts reported in *Hellar*,²⁷⁴ only a short time elapsed from the moment the bartender was notified and asked to remove the defamatory script and the time when the script was found still on the wall later that evening. This period was deemed sufficient to create a jury question as to "republication."²⁷⁵ On the contrary, *Tackett v. General Motors Corp.*²⁷⁶ held that a longer period of time—three days—did not amount to republication. Someone painted an allegedly defamatory sign on an inside wall of a General Motors Plant, and an employee brought a defamation action against the employer for, inter alia, failing to remove it. The court affirmed the lower court's directed verdict for the regarding this painted sign.²⁷⁷ Although recognizing that failure to remove a libel from a building after notice and opportunity to do so is a form of adoption of the publication, the court held that the limited period of time would ban any recovery in this case.²⁷⁸ In fact, when the burden of constant vigilance greatly exceeds the expected benefits, such benefits are to be evaluated on the basis of the probability that a reader will infer that the statement has been adopted. The court held that three days was an insufficient period of time for this purpose.²⁷⁹

The *Restatement of Torts* supports the rule that a failure to remove harmful matter from a medium of communication such as a bulletin board constitutes republication for which the republisher may be liable.²⁸⁰ The *Restatement* asserts that "[o]ne who intentionally and unreasonably fails to remove defamatory matter that he knows to be exhibited on land or chattels in his possession or under his control is subject to liability for its continued publication."²⁸¹ Under this standard, a sysop would face liability if it or its agent "intentionally and unreasonably" failed to control the content of the materials published on the system.

F. Sysop's Liability: A Tentative Conclusion

In the attempt to draw a conclusive stand on the possible law governing sysop's liability, *Cubby v. CompuServe*²⁸² and *Stratton Oakmont, Inc. v. Prodigy Services Co.*²⁸³ are the key cases. However, it is necessary to move some steps beyond these cases and shed some light on untapped territories by use of analogies. An activity that on its face should alert a reasonably prudent sysop, and that should induce the sysop to ban it from the system to avoid harm and injuries, may be scrutinized within the framework proposed in *Braun v. Soldier of Fortune*.²⁸⁴ On a case-by-case analysis, important issues are whether the service user is a public or a private figure, and whether the *Gertz* standard (as indirectly modified by subsequent decisions) applies.

Limiting sysop's liability to cases where they have knowledge of the existence of the harmful messages or activities would preserve freedom of expression on computer networks.²⁸⁵ The knowledge standard would apply when a sysop himself posted a harmful message or failed to remove a message posted by system users. Analogies to the standards applied to republishers and bulletin boards support this analysis and offer useful guidelines for the future regulation of cyberspace.

Once the knowledge requirement has been assessed, the *Smith*²⁸⁶ and *Fogg*²⁸⁷ cases provide some clear guidelines to help us strike a balance between that requirement and the burden imposed on the sysop and free expression. The *Smith* standard,²⁸⁸ which requires that the republisher/distributor have knowledge of the harmful contents of the material to be held liable for it, alleviates the sysop's responsibility to read all information before it is posted. The *Smith* rationale can be applied to system operators of all sizes, because it is hinged on the response of the system's users. If the users complain, the sysop would be required to intervene and remove the harmful message.²⁸⁹ If no users complain, then the system will automatically adapt itself to a new community standard. At the same time, by excluding a strict liability standard, *Smith* protects the basic activity of the sysops, thus erecting a solid barrier in defense of the flow of constitutionally-protected speech and of new ideas.

The *Fogg* rule,²⁹⁰ which states that failure to remove harmful messages can amount to having endorsed or ratified the posting (republication),²⁹¹ suggests two main implications for sysop liability. The first is that liability should depend on how closely the allegedly harmful message or activity is related to the business fostered by the sysop.²⁹² For example, a sysop providing specialized services to the legal community would be held to a specific standard of care adequate to the protection of the interests involved. If the harm is peripheral to the function of the system (for example, if the conferencing features of the system are mixed up with junk mail), the user is sufficiently protected by the option to switch to a similar service provided by a different sysop. In contrast, a sysop who establishes an electronic bulletin board for a law firm permitting clients and lawyers to transmit and receive files would be required to provide special protection. Any illegal conduct carried out on such specialized systems is likely to cause much greater harm than on generic systems, and the sysop should be held to a higher standard of care.

The second implication of the *Fogg* rule is that constructive knowledge can be imputed to the sysop when he or she has received notice of the harmful message.²⁹³ In cases like *CompuServe* and *Prodigy*, where a third party controls the contents of any publication, sysops should be aware of the consequences of the acts of their agents. The *Fogg* rule indicates that they can be estopped from denying the ostensible or apparent authority that caused the harm in question.²⁹⁴

Under the rules suggested by the relevant cases, then, the standard of sysop liability is negligence rather than strict liability.²⁹⁵ Moreover, since an ordinary negligence standard (like the one in *Gertz*) would impose an intolerable burden on bulletin board operators, most of whom lack the resources to engage in extensive prescreening of submitted material, the standard must include an actual knowledge requirement. The advantages of adopting such a standard are multiple. Negligence under this standard depends on the function actually performed by the sysop and on the sysop's status (commercial versus hobbyist). In general, commercial sysops would be held to a higher standard of care, mitigated by a risk-utility balancing test, whereas hobbyist sysops would be held to a lesser standard. Additionally, a negligence standard can more easily evolve over time as the technology or industry practices change. The standard of care may come to include monitoring or other sorts of affirmative duties, depending on how the industry evolves.²⁹⁶

V. Computer Systems, Public Fora and Policies

The public forum doctrine provides another angle on the question of the regulation of speech on computer systems. Public property

which has traditionally been the site of a free exchange of ideas, or which has been intentionally opened to public speech, is covered by the doctrine.²⁹⁷ In *Hudgens v. NLRB*,²⁹⁸ the Supreme Court held that "a municipality may not . . . discriminate in the regulation of expression on the basis of the content of that expression."²⁹⁹

Although the public forum doctrine applies mainly to sites owned by the government, it has been extended in some situations to apply to private property. For example, *Marsh v. Alabama*³⁰⁰ established that a privately-owned company town became the functional equivalent of a public municipality when it took on all the attributes of a town (i.e., a town's policeman, residential buildings, streets, sidewalks, a system of sewers, a sewage disposal plant and a business district) and was accessible to and freely used by the general public.

The public forum doctrine opens a new perspective on the potential rights of users to communicate through and on a computer system, even against the system operator's permission. Are computer systems public or private fora? Can a claim of First Amendment violation by regulations that limit the right of access still be considered?

In many ways, computer networks resemble public fora because of their large size, accessibility and open use. However, they do not have a long-standing dedication to public discourse, and access to them is generally regulated by a contractual relationship between the sysop and the user.³⁰¹ Some computer networks, however, are open to the general public. Those run by cities and federal agencies represent public services designed to facilitate public communication, and users may expect autonomy and free access.³⁰² Consequently, the application of the public forum doctrine to sysops can be determined on a case-by-case basis.

Those bulletin boards and networks which require a subscription contract for access cannot be accorded the special status of public fora. Nevertheless, the economic analysis which underlies the public forum doctrine may supply useful parameters for future regulation of the industry.

Economists view a public forum as a form of subsidy. Whenever the government provides speakers with the use of certain fora, the public forum doctrine creates an entitlement in favor of any speaker, preventing any kind of discrimination or paternalism.³⁰³ Since computer networks also make speech cheaper, this analysis supports making some public forum-like right available in the on-line world. Users without alternative channels of communication may be entitled to use the computer system as long as they do not impose an undue cost on the sysop. In this case, a direct protection of Internet users is probably available even absent state regulations that guarantee their rights.

VI. Conclusion

A fundamental consideration when dealing with operators of computer systems is that they provide a service that facilitates communication by the users themselves. The information on the networks is generally created and propagated by the users themselves. Sysops may find themselves vicariously liable for the actions of the system's users. It is important that the boundaries of sysop liability be clarified so that sysops may eliminate or reduce harm when they can, and so that the provision of network access is not overdeterred.

The economic analysis touched upon above makes manifest the need for such clarity. Economists classify information as a "public good."³⁰⁴ Once information is made available, it can be readily transmitted to the public at large which enjoys its benefits. The public, however, does not pay for the benefits received from information. "Individuals have an incentive to 'free ride' because they can enjoy the benefits of public goods without helping to produce those goods."³⁰⁵ Thus, information cannot be valued on the basis of market demand or willingness and ability to pay. Rather, it "is likely to be undervalued by both the market and the political system."³⁰⁶ If market demand for information reflects only the benefits to purchasers and not also the benefits received by free riders, then the demand appears to be substantially lower than the real level of utilization. Accordingly, markets may tend to reduce their production of information because most people do not pay for it, and because the apparent demand for it is low.

"[T]his undervaluation of information requires special constitutional protection for information-related activities."³⁰⁷ However, regulating information is a delicate process, which can easily reflect prejudice or ideology. This makes information "especially vulnerable in the political process [of regulating it], precisely because it has the attributes of a public good."³⁰⁸ Therefore, "if the government intervenes in the market at all, it should subsidize speech rather than limit it."³⁰⁹

If the sysop is an information provider, its recovered benefit will not reflect the full social value of the publication. Thus the sysop cannot internalize all the benefits of the business, though it must internalize all the costs, which necessarily include potential tort liability. Thus, costs are constantly higher than benefits.

One possible solution to this problem is to limit the sysop's tort liability.³¹⁰ In fact, if sysops were indiscriminately liable for all activities, they would have to strike a balance between the costs of harmful information and the benefits of producing additional "safe" information. In many cases, this would force sysops to raise the prices of their services. But in many other instances, sysops would adopt the more radical remedy of interrupting their information service. To prevent this overdeterrence, the legal system should provide the sysop considerable protection against liability.³¹¹

Another possible approach is to create a public forum-like rights in the computer network context, to guarantee access to systems for all speakers. The effect of such rights would be to provide a subsidy, at the expense of the sysops, for speech over the network. However, this right should be limited to situations where there were no alternative channels of communication for the speaker, and the speech would not significantly impact the sysop's operation or costs.

Computer systems can beneficially affect both the communication of information and information itself. Moreover, "the speed and cost-effectiveness of computer systems can lead to the instantaneous and low-cost formation of interest-based groups, without regard to any user's geography or demographic characteristics."³¹² The knowledge and the exchange of diverse information benefits the development of a cosmopolitan society whose members recognize the value of their individual cultures and traditions and learn how to interact with different cultures and traditions. Such knowledge represents the fountainhead of any future beneficial development of different archetypal models affecting old and modern societies. An individual may log onto a computer network, or even start up her own computer bulletin board, with a minimum investment of money or time. Even in the absence of any regulations, users enjoy the status of hearers and providers of information at the same time. As long as gatekeepers of communication channels defend the existence of an overall diversity of communication means, and avoid their unfair exploitation as well,³¹³ there is no apparent need to correct any distortion of the marketplace.³¹⁴ In the powerful words of Justice Holmes, "the best test of truth is the power of the thought to get itself accepted in the competition of the market."³¹⁵ The computer network industry may well promote the free marketplace of ideas that Justice Holmes had in mind.

†1996 Giorgio Bovenzi.

† M.C.J., 1995, New York University of Law; J.D., 1988, University of Naples Law School. Mr. Bovenzi, a member of the Italian bar, is currently clerking for the Honorable Donald C. Pogue at the U.S. Court of International Trade, New York. The author wishes to thank Professor Richard H. Levenson of New York University School of Law for his many helpful corrections and valuable comments on prior drafts of this paper.

1. See RAFFAELE AJELLO, *STORIA DEL DIRITTO ITALIANO* (1984); FRANCESCO SALVIOLI, *STORIA DEL DIRITTO ITALIANO* (1950); see also DOUGLAS C. MCMURTRIE, *THE BOOK: THE STORY OF PRINTING AND BOOK MAKING* 67 (1943).
2. MCMURTRIE, *supra* note 1, at 61.
3. See generally Annotation, *Questions of Evidence Involved in the Inspection and Examination of Type-written Documents and Typewriting Machines*, 106 A.L.R. 721 (1937).
4. BENJAMIN WRIGHT, *THE LAW OF ELECTRONIC COMMERCE* 267-68 (1994 Supp.).
5. Cf. *Losses and Market Changes Prompt Audition to Examine Internal Controls*, BANKING REP. (BNA), Jan. 29, 1996, at 133.
6. For a general introduction to legal issues in cyberspace, see EDWARD A. CAVAZOS & GAVINO MORIN, *CYBERSPACE AND THE LAW: YOUR RIGHTS AND DUTIES IN THE ON-LINE WORLD* (1994). More detailed materials are in BENJAMIN WRIGHT, *THE LAW OF ELECTRONIC COMMERCE: EDI, E-MAIL AND INTERNET: TECHNOLOGY, PROOF, AND LIABILITY* (2nd ed. 1995); PETER B. MAGGS & JAMES A. SPROWL, *COMPUTER APPLICATIONS IN THE LAW* (1987); RICHARD RAYSMAN & PETER BROWN, *COMPUTER LAW: DRAFTING AND NEGOTIATING FORMS AND AGREEMENTS* (1995).

For a general description of an office environment organized around digital computer applications see HENRY H. PERRIT, JR., *HOW TO PRACTICE LAW WITH COMPUTERS* (1992).

For a more technical but very pragmatic orientation to the exploitation of new technologies in the practice of the legal profession, see

V. MITAL & L. JOHNSON, *ADVANCED INFORMATION SYSTEMS FOR LAWYERS* (1992). The book contains a description of various specific areas in which advanced information systems are used by lawyers, including document drafting and assembly, litigation support, neural networks for legal reasoning and information retrieval.

7. Even though the means used to commit a tort can be relevant to levels of liability and the consequent damages, it seems irrelevant whether the agent utilized a mechanical or an electronic means. A different question is whether it is important to distinguish between the intention to do an act that causes harm, and the intention to cause harm. *See, e.g.*, RICHARD A. EPSTEIN ET AL., *CASES AND MATERIALS ON TORTS* 3 (1985). The common law of torts provides for those distinctions in connection with different torts.

8. The standard of liability referred to here is the negligence standard, which seems appropriate, for the reasons discussed below. The negligence standard is based on (1) a duty or obligation that the defendant owed the plaintiff to conform his conduct in order to prevent an unreasonable risk of harm, (2) a breach of that duty or obligation, (3) a causal connection between the defendant's breach and the plaintiff's harm, and (4) a damage or injury caused by the breach. EPSTEIN, *supra* note 7, at 119-20.

9. In this case, the doctrine of proximate causation detects which of these actions severs the causal connection between the injury and the conduct. The doctrine indicates two possible tests, one based on the foreseeability or probability of the chain of events, the other on the interruption of the causal connection by one of the parties. EPSTEIN, *supra* note 7, at 309-50.

10. *See generally* EPSTEIN, *supra* note 7, at xxxi-xxxv.

11. The potential liability of computer system operators for copyright infringement will be discussed only briefly in this article.

12. For good comprehensive guides on the Internet, see DANIEL P. DERN, *THE INTERNET GUIDE FOR NEW USERS* (1994) (a thorough and informative reference for beginners and experienced users, clear and easy to consult); PHILIP BACZEWSKI ET AL., *THE INTERNET UNLEASHED* (1994); PAUL GILSTER, *THE INTERNET NAVIGATOR* (1994).

For a detailed guide to electronic journals, newsletters, electronic books, libraries and databases on the Internet, see DAVID F.W. ROBINSON & JONATHAN KOCHMER, *THE INTERNET PASSPORT: NORTHWESTNET'S GUIDE TO OUR WORLD ONLINE* (1995). The book also contains information on health care and medical science resources, genetics and molecular biology, together with a description of supercomputer sites (even though limited to the NorthWest area).

13. TCP/IP is suitable for the interconnection of heterogeneous packet networks.

14. Telnet, File Transfer Protocol, E-mail, WAIS and Gopher are among the common programs used to facilitate inter-system communication. The Telnet program allows a user on one computer to connect to a remote machine as if it were a local one. File Transfer Protocol (FTP) allows the transfer of files from one computer to another between Internet systems. E-mail programs send correspondence from one personal account to any Internet machine. WAIS and Gopher let users search indices of information distributed by host systems. *See generally* DERN, *supra* note 12. The World-Wide Web (Web) allows the user to follow hypertext links which cross reference many sources of information, including text, sounds and images. The Web was invented at CERN, the European Laboratory for Particle Physics (Geneva, Switzerland), and it is described by Tim Berners-Lee, its inventor, as "a large-scale networked hypertext information system" and "an embodiment of human knowledge" that is stored around the world and accessed through computers connected to the Internet. A collection of computers on the Internet makes a wide variety of information easily available to anyone. The Web includes the other services in the sense that it allows access to Gopher and the transfer of files using FTP. Tim O'Connor, *Lynx Provides Easy Access to the World-Wide Web on the Internet*, *ACAD. COMPUTING AND NETWORKING AT N.Y.U.*, Sept. 1994, at 5.

15. During 1995, the number of direct World Wide Web users grew from one million to eight million. Jared Sandberg & Bart Ziegler, *Web Trap: Internet's Popularity Threatens to Swamp the On-line Services*, *WALL. ST. J.*, Jan. 18, 1996, at A1, A6.

16. *See generally* GILSTER, *supra* note 12.

17. America Online Inc. counts more than five million members. Thomas E. Weber, *AOL's Revenue Grew Threefold in 2nd Quarter*, *WALL ST. J.*, Feb. 7, 1996, at B5. The commercial on-line services combined have grown to about 12.5 million subscribers. Sandberg & Ziegler, *supra* note 15, at A1, A6.

18. GILSTER, *supra* note 12, at 78-79.

19. *See generally* GILSTER, *supra* note 12.
20. Cities, states and federal agencies run BBSs as public services. There is a BBS on any topic of interest, from the sale of second-hand records to right-wing extremist propaganda.
21. *See* GILSTER, *supra* note 12, at 292-93.
22. *See* GILSTER, *supra* note 12, at 327-30.
23. *See generally* DERN, *supra* note 12.
24. The constitutional right of privacy protects personal privacy against unlawful government invasion. 62A AM. JUR. 2D *Privacy* § 8 (1990). This right corresponds, at the community level, to the right to associate with other people in pursuit of a wide variety of ends. *Cf. Roberts v. United States Jaycees*, 468 U.S. 609 (1984) (noting that constitutional protection of the individual's choice to enter into and maintain certain intimate or private relationships, and the freedom of individuals to associate in order to engage in protected speech, represent two principles both contained in the First Amendment). The First Amendment provides in relevant part: "Congress shall make no law . . . abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. CONST. amend. I.
25. 62A AM. JUR. 2D *Privacy* § 8 (1990).
26. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960). The intrusion must be highly offensive, but no publication to others is necessary (e.g., reading someone's private correspondence, or surreptitiously gaining access to someone's data or files satisfies the standard). See RESTATEMENT (SECOND) OF TORTS § 652B (1977) (Intrusion upon Seclusion), which follows Prosser's classification, and has also been adopted by many courts. See also RESTATEMENT (SECOND) OF TORTS § 652B illus. 3 (1977), which involves a private detective, A, seeking evidence for use in a lawsuit involving B without B's knowledge. The illustration reads in relevant part: "A taps B's telephone wires and installs a recording device to make a record of B's conversations. A has invaded B's privacy." Other examples of the tort of invasion of privacy are the public disclosure of embarrassing private facts, publicity that places someone in a false light in the public eye and the appropriation of someone's name or likeness. *See* Prosser, *supra* at 387; RESTATEMENT (SECOND) OF TORTS §§ 652D, 652E (1977). The defense of "newsworthiness" has received a broad construction in invasion of privacy cases, where courts have been anxious to avoid conflict between the private tort action and the constitutional guarantees of freedom of speech and of the press. *See Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469, 496 (1975) (holding that the First and Fourteenth Amendments do not impose liability on the press for truthfully publishing information released to the public in official court records).
27. *Rhodes v. Graham*, 37 S.W.2d 46, 47 (Ky. 1931) (holding that allegation that phone conversations were overheard by means of tapping of a telephone line stated a cause of action for damages).
28. *Moore v. New York Elevated R.R. Co.*, 29 N.E. 997, 998 (N.Y. 1892).
29. *Birnbaum v. United States*, 588 F.2d 319, 326 (2d. Cir. 1978) (holding that the plaintiff stated a cause of action against the CIA when the agency covertly opened and read first-class mail sent between American citizens and the Soviet Union).
30. *Roach v. Harper*, 105 S.E.2d 564, 568 (W.Va. 1958) (allowing an action for invasion of privacy when the defendant used a "hearing device" to overhear the plaintiff's private and confidential conversations in an apartment that he rented to her).
31. The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2701 (1986), protects the content of any stored communication. *See infra* part III.C.3.
32. *See* John T. Soma & Lorna C. Youngs, *Confidential Communications and Information in a Computer Era*, 12 HOFSTRA L. REV. 4 (1984). The Electronic Communications Privacy Act does not define what is "private" or what constitutes an "authorization." Many sysops post some kind of disclaimer, either as a bulletin or as part of a service contract, formal or implied, that no "private" mail exists on their system. Notwithstanding any disclaimer, almost all mail software treats some messages as "private."

33. Encryption keys are numbers that are plugged into a mathematical algorithm and used to scramble data. By doing this, the original sequence of binary digits (the 1s and the 0s that make a digital file) is scrambled into a new sequence of binary digits; this new string represents the encrypted work.

Recently, a new cryptography system based on the public key algorithm has been introduced. In a public key system, each message requires two keys. One is a public and can be distributed to anyone who wants it, and the other is private. Only the holder of the private key can decrypt the message.

34. However, the routine use of cryptography is not only expensive but also slows communication.

35. RESTATEMENT (SECOND) OF TORTS § 652A cmt. c (1977).

36. *See supra* note 24.

37. 362 U.S. 60 (1960).

38. *Id.* at 60-61.

39. *Id.* at 65.

40. 115 S. Ct. 1511 (1995).

41. *Id.* at 1524. In *Hurley v. Irish-American Gay, Lesbian and Bisexual Group of Boston*, 115 S. Ct. 2338, 2347 (1995), the Supreme Court explained that freedom of speech applies also to "statements of fact the speaker would rather avoid."

42. 357 U.S. 449 (1958).

43. *Id.* at 462.

44. 372 U.S. 539 (1963).

45. *Id.* at 549.

46. *Id.* at 557-58.

47. The recipient can respond using the assigned code.

48. This doctrine, a tentative application of the protection under the right of assembly to on-line users, is justified by "the sense of community that develops in some on-line situations [which] resembles an association for purposes of constitutional law analysis." CAVAZOS & MORIN, *supra* note 6, at 15. However, so far no court has faced such a case, and therefore there are no precedents on point.

49. 18 U.S.C. §§ 2510-2521 (1994).

50. Pub. L. No. 103-414, § 101, 108 Stat. 4279 (1994) (codified as 47 U.S.C. § 1001 *et seq.* (1994)).

51. Pub. L. No. 104-104, § 502, 110 Stat. 56 (1996).

52. These defenses are intended to limit sysop's vicarious liability under the Act.

53. Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2520 (1968)). Upon enacting the law, Congress found that there had been extensive wiretapping carried on without legal sanction and without the consent of any of the parties to the conversation, and that these activities infringed upon the privacy of wire and oral communications as well as upon the integrity of

court and administrative proceedings.

54. 18 U.S.C. § 2511 (1994).

55. 18 U.S.C. § 2520(a) (1986).

56. 18 U.S.C. § 2520(b) (1986).

57. 18 U.S.C. § 2511(2)(a)(i) (1994).

58. 18 U.S.C. § 2511(2)(a)(ii) (1994).

59. 18 U.S.C. § 2511(2)(h) (1994).

60. 18 U.S.C. § 2511(3)(a) (1994).

61. 18 U.S.C. § 2511(3)(b) (1994).

62. 18 U.S.C. § 2511(2)(b) (1994).

63. 18 U.S.C. § 2511(2)(c) (1994).

64. 18 U.S.C. § 2702(a) (1988).

65. 18 U.S.C. § 2703 (1994).

66. 18 U.S.C. § 2703(c)(1)(B) (1994) (mandating a sysop to disclose a record to a government entity only when the procedures have been followed); 18 U.S.C. § 2703(e) (1994) (denying cause of action against a sysop disclosing information under this chapter). Therefore, a cause of action exists against the sysop if the sysop disclosed information to a government entity that did not follow the appropriate procedures.

67. 18 U.S.C. § 2703 (1994).

68. 47 U.S.C. § 1001 *et seq.* (1988 & Supp. 1993).

69. H.R. REP. NO. 827, 103rd Cong., 2d Sess. part I, at 9 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3493.

70. 47 U.S.C. § 1002(a) (1994). As noted in the House Report, only recently has the question of system design become an issue. H.R. REP. NO. 827, *supra* note 69, at 9, *reprinted in* 1994 U.S.C.C.A.N. at 3493. New technologies and services have complicated law enforcement's task. *Id.* at 3494. In a hearing on March 18, 1994, the FBI director testified that the Federal Bureau "had identified specific instances in which law enforcement agencies were precluded due to technological impediments from fully implementing authorized electronic surveillance." *Id.*

71. 47 U.S.C. § 1002(b)(2) (1994). Information services are defined as services offering a "capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications," and include electronic publishing and electronic messaging services. 47 U.S.C. § 1001(6) (1994). Information services and private networks, therefore, both fit in the category of sysops as defined in this article. The House Report clarifies that "all information services, such as Internet service providers or services such as Prodigy and America On-line," are excluded from the Act's coverage. Therefore, "these services and systems do not have to be designed so as to comply with the capability requirements." H.R. REP. NO. 827, *supra* note 69, at 9, *reprinted in* 1994 U.S.C.C.A.N. at 3498.

72. *See* 47 U.S.C. § 1002(a) (1994) *See also* H.R. REP. NO. 827, *supra* note 69, at 9, *reprinted in* 1994 U.S.C.C.A.N. at 3497. The standard now imposed is not a probable cause standard, but an intermediate one, to protect on-line transactional records. Under this standard, the court must find, based on law enforcement's showing of facts, that there are specific and articulable grounds to believe

that the records are relevant and material to an ongoing criminal investigation. A subpoena can still be used to obtain the name, address, telephone toll billing records and length of service of a subscriber or customer, and the types of services the subscriber or customer utilized.

73. 47 U.S.C. § 1002(b)(3) (1994). Telecommunications carriers have no responsibility to decrypt encrypted communications that are the object of court-ordered wiretaps, unless the carrier provided the encryption and can decrypt it. *Id.*

74. Pub. L. No. 103-414, § 202(a) (1994). The amended provisions of the ECPA are those contained in 18 U.S.C. § 2510(1), (12) (1994).

75. Services like PBXs or ATM networks, which support private networks or telecommunications carriers, are excluded. H.R. REP. NO. 827, *supra* note 69, at 18, *reprinted in* 1994 U.S.C.C.A.N. at 3498. *See also supra* note 71. However, access to a network is commonly through a dial-in connection to a host computer using a standard phone line, a personal computer and a modem. In this case, the communication can be intercepted at the telecommunications carrier before it is switched into the private network.

76. H.R. REP. NO. 827, *supra* note 69, at 50, *reprinted in* 1994 U.S.C.C.A.N. at 3515.

77. *Id.* at 3493. Several provisions in the Act are intended to ease the burden on the industry. A four-year transition is granted to telephone companies and other entities during which they can make any necessary changes in their facilities. Pub. L. No. 103-414, § 111(b) (1994). Furthermore, the federal government will pay reasonable costs incurred by industry in retrofitting facilities to correct existing problems. 47 U.S.C. § 1008(a) (1994). Law enforcement agencies may not dictate system design features and may not bar introduction of new features and technologies. 47 U.S.C. § 1002(b)(1) (1988 & Supp. 1993). The industry itself shall decide how to implement law enforcement's requirements, by establishing publicly available specifications creating "safe harbors" for carriers. 47 U.S.C. §§ 1005, 1006 (1988 & Supp. 1993).

78. Pub. L. No. 104-104, §§ 501-561, 110 Stat. 56, 132-43 (1996) (to be codified at 47 U.S.C. §§ 223).

79. Pub. L. No. 104-104, 110 Stat. 56 (1996) (codified as amended in scattered sections of 47 U.S.C.).

80. 47 U.S.C. § 201 *et seq.* (1988 & Supp. 1993).

81. Pub. L. No. 104-104, § 502, 110 Stat. 56, 133 (to be codified at 47 U.S.C. § 223(a)(1)(C)).

82. Pub. L. No. 104-104, § 502, 110 Stat. 56, 133 (to be codified at 47 U.S.C. § 223(a)(1)(E)).

83. Pub. L. No. 104-104, § 502, 110 Stat. 56, 133 (to be codified at 47 U.S.C. § 223(a)(1)(A)).

84. Pub. L. No. 104-104, § 502, 110 Stat. 56, 133 (to be codified at 47 U.S.C. § 223(a)(1)(B)).

85. Pub. L. No. 104-104, § 502, 110 Stat. 56, 133-34 (to be codified at 47 U.S.C. § 223(a)(2)).

86. *Id.*

87. An interactive computer service is defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." Pub. L. No. 104-104, § 509, 110 Stat. 56, 138 (to be codified at 47 U.S.C. § 230(e)(2)).

88. Pub. L. No. 104-104, § 502, 110 Stat. 56, 133-34 (to be codified at 47 U.S.C. § 223(d)).

89. Pub. L. No. 104-104, § 502, 110 Stat. 56, 134 (to be codified at 47 U.S.C. § 223(d)(2)).

90. FCC v. Pacifica Found., 438 U.S. 726, 732 (1978); S. CONF. REP. NO. 230, 104th Cong., 2nd Sess. 188 (1996).

91. S. CONF. REP. NO. 230, *supra* note 90, at 189.

92. *Id.*

93. Pub. L. No. 104-104, § 502, 110 Stat. 56, 134 (to be codified at 47 U.S.C. § 223(e)(1)).

94. *Id.*

95. Pub. L. No. 104-104, § 502, 110 Stat. 56, 134 (to be codified at 47 U.S.C. § 223(e)(2)).

96. Pub. L. No. 104-104, § 502, 110 Stat. 56, 134 (to be codified at 47 U.S.C. § 223(e)(3)).

97. S. CONF. REP. NO. 230, *supra* note 90, at 190.

98. Pub. L. No. 104-104, § 502, 110 Stat. 56, 134 (to be codified at 47 U.S.C. § 223(e)(4)).

99. Pub. L. No. 104-104, § 509, 110 Stat. 56, 138 (to be codified at 47 U.S.C. § 230(c)).

100. Pub. L. No. 104-104, § 502, 110 Stat. 56, 134 (to be codified at 47 U.S.C. § 223(e)(5)(A)).

101. S. CONF. REP. NO. 230, *supra* note 90, at 190.

102. Pub. L. No. 104-104, § 502, 110 Stat. 56, 134 (to be codified at 47 U.S.C. § 223(e)(5)(B)).

103. Pub. L. No. 104-104, § 502, 110 Stat. 56, 134-35 (to be codified at 47 U.S.C. § 223(e)(6)).

104. *Id.* This subsection "should be narrowly construed" in that no further authority over interactive computer services is granted to the FCC. S. CONF. REP. NO. 230, *supra* note 90, at 191.

105. Pub. L. No. 104-104, § 502, 110 Stat. 56, 135 (to be codified at 47 U.S.C. § 223(f)(2)).

106. *Id.*

107. S. CONF. REP. NO. 230, *supra* note 90, at 191.

108. *ACLU v. Reno*, No. 96-963, 1996 U.S. Dist. LEXIS 1617, *1-3 (E.D. Pa. Feb. 15, 1996). Among the groups joining the *ACLU* in the action were the Electronic Frontier Foundation, the Human Rights Watch, the National Writers Union and the Journalism Educational Association.

109. *Id.* at *3.

110. *Id.*

111. *Id.* at *5, *6.

112. *Id.* at *6.

113. *Id.* at *8. Pub. L. No. 104-104, § 502, 110 Stat. 56, 133-34 (to be codified at 47 U.S.C. § 223(d)) covers any "communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs."

114. *2nd Major Court Challenge To Telecom Act Filed*, COMMS. DAILY, Feb. 27, 1996, at 2 [hereinafter COMMS. DAILY]. Among the plaintiffs are America Online, the American Library Association, Apple Computer Inc., Microsoft Corp., Prodigy Services Co.,

Meanwhile, under the pressure created by the enactment of the CDA, Microsoft Corp. has endorsed RSAC-I, a worldwide ratings system for on-line information designed to enable parents and teachers to screen communications for violence, sexual themes and offensive language. Microsoft's implementation of RSAC-I would offer the option of blocking access to any Web site not provided with the ratings system. Peter H. Lewis, *Microsoft Backs Ratings System For The Internet*, N.Y. TIMES, Mar. 1, 1996, at D1.

115. COMMS. DAILY, *supra* note 114.

116. *See Miller v. California*, 413 U.S. 15, 32-33 (1973).

117. 39 U.S.C. § 3008 (1994).

118. *Id.*

119. 39 U.S.C. § 3008(a) (1994).

120. 39 U.S.C. § 3008(b) (1994).

121. 39 U.S.C. § 3008(c) (1994).

122. 397 U.S. 728 (1970).

123. *Id.* at 740.

124. *Id.* at 737.

125. The Postal Reorganization Act of 1970 transformed the Post Office Department into a government-owned corporation called the United States Postal Service. Former 39 U.S.C. § 4009 (1964) referred to the Postmaster General whereas 39 U.S.C. § 3008 (1994) refers to the Postal Service. But for this difference, the provisions have not been altered.

126. 397 U.S. at 734-37 (emphasis added).

127. *Id.* at 736.

128. 319 U.S. 141 (1943).

129. *Id.* at 149.

130. *Id.* at 146-47.

131. *Id.* at 148.

132. *Id.* In *Camara v. Municipal Court of San Francisco*, 387 U.S. 523 (1967), the Supreme Court gave substantial ground to the constitutional protection of privacy. This was an action by a lessee of an apartment to prohibit his prosecution for refusing to permit warrantless inspection of his premises. Justice White for the Court held that such searches, without a warrant, lack traditional safeguards which the Fourth Amendment guarantees to individuals. The principle can certainly be extended to cover a general protection of the individual and his private property. In fact, as the Court noted, it would be

anomalous to say that [rights] . . . are fully protected by the Fourth Amendment only when the individual is suspected of criminal behavior, . . . [because] even the most law-abiding citizen has a very tangible interest in limiting the circumstances under which the sanctity of his home may be broken by official authority, for the possibility of criminal entry under the guise of official sanction is a serious threat to personal and family security.

Id. at 530-31.

133. The Postal Service must order the sender to refrain from further mailings, and to delete the name of the designated addressee from all mailing lists. *See supra* text accompanying notes 114 & 115.

134. 18 U.S.C. §§ 2510-2521 (1994).

135. A flame, in Net jargon, is an insult or provocation that is either posted or e-mailed.

136. *See generally* 50 AM. JUR. 2D *Libel and Slander* §§ 2, 6 (1995).

137. *See* RESTATEMENT (SECOND) OF TORTS §§ 652A-652I (1977).

138. *See generally* 16A AM. JUR. 2D *Constitutional Law* §§ 440-446, 457 (1979). However, some state constitutions extend this protection to their citizens not only against the activity of the state and the local government, but also against the activity of other individuals.

139. 50 AM. JUR. 2D *Libel and Slander* § 30 (1995).

140. *Id.*

141. *Id.* at § 13 (1995).

142. The issue has been considered by legal scholars. *See, e.g.,* Loftus E. Becker, Jr., *The Liability of Computer Bulletin Board Operators for Defamation Posted by Others*, 22 CONN. L. REV. 203 (1989).

143. *See* 50 AM. JUR. 2D *Libel and Slander* §§ 21-28 (1995).

144. The plaintiff must also prove that there has been defamatory language aimed at or referring to the plaintiff with some degree of specificity. The defamatory language must be untrue and nonconsensual. Opinions of the speaker cannot be defamatory unless they contain specific factual allegations. Finally, the identity of the defamed party must be clear to the audience. 50 AM. JUR. 2D *Libel and Slander* §§ 106, 107, 110-116 (1995).

145. The plaintiff must establish the damages resulting from the defamatory communication. In some cases involving private figures, *presumed* damages are allowed. 50 AM. JUR. 2D *Libel and Slander* §§ 374-377 (1995).

146. 376 U.S. 254 (1964).

147. *Id.* at 264.

148. *Id.* at 280.

149. *Id.* at 270; *See also* 50 AM. JUR. 2D *Libel and Slander* § 42 (1995).

150. 376 U.S. at 272-73.

151. *Id.*

152. 62A AM. JUR. 2D *Privacy* § 190 (1990).

153. 418 U.S. 323 (1974).

154. *Id.* at 347 (emphasis added).

155. *Id.* at 349.

156. *Id.*

157. *Id.*

158. *Id.* at 344 (footnote omitted).

159. *Id.* at 345.

160. 472 U.S. 749 (1985).

161. *Id.* at 759.

162. *Id.* at 761.

163. 485 U.S. 46 (1988).

164. *Id.* at 48.

165. *Id.* at 56-57.

166. Even though becoming a public figure generally involves an act of deliberate will, a person can become a public figure when she adopts conduct which solicits public attention. *See* 50 AM. JUR. 2D *Libel and Slander* § 72 (1995).

167. The analysis of what constitutes "public concern" would force the discussion to completely different fields. Indeed, a distinction can be made whether "public concern" is such because it is (objectively) public or because it is (subjectively) of concern to a number of people.

168. Litigation involving the right of privacy based on the plaintiff's status as a public figure has included not only public officials and candidates for public offices, but also anybody remotely likely to receive public attention. *See* 62A AM. JUR. 2D *Privacy* § 194 (1990).

169. 62A AM. JUR. 2D *Privacy* § 194 editor's observation (1990).

170. It may be observed that this is the reality for everything else in modern public communication.

171. 776 F. Supp. 135 (S.D.N.Y. 1991).

172. *Id.* at 137.

173. *Id.* at 137-38.

174. *Id.* at 137.

175. *Id.*

176. *Id.*

177. *Id.*

178. *Id.* at 138.

179. *Id.* at 139 (citing *Cianci v. New Times Publishing Co.*, 639 F.2d 54, 61 (2d Cir. 1980) quoting RESTATEMENT (SECOND) OF TORTS § 578 (1977): "Except as to those who only deliver or transmit defamation published by a third person, one who repeats or otherwise republishes defamatory matter is subject to liability as if he had originally published it.").
180. *Id.* at 139. (citing *Lerman v. Chuckleberry Publishing, Inc.*, 521 F. Supp. 228, 235 (S.D.N.Y. 1981) and *Macaluso v. Mondadori Publishing Co.*, 527 F. Supp. 1017, 1019 (E.D.N.Y. 1981)).
181. *Id.* at 139 (citing *Smith v. California*, 361 U.S. 147 (1959)). This case will be analyzed shortly in part IV.E.3.
182. *Id.* at 140.
183. *Id.* at 140.
184. Under the contract between CompuServe and CCI, the latter agreed "to manage, review, create, delete, edit and otherwise control the contents of the [Journalism Forum], in accordance with editorial and technical standards and conventions of style as established by CompuServe." *Id.* at 143.
185. *Id.*
186. *Id.*
187. *Id.*
188. *Id.*
189. Plaintiff Cubby sued CompuServe and Fitzpatrick (DFA), but not Cameron Communications (CCI).
190. No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995) (Stuart L. Ain, J.) (unpublished).
191. "Prodigy contracts with bulletin board leaders, who, among other things, participate in board discussions and undertake promotional efforts" to attract users. *Id.* at *1.
192. "Money Talk" is allegedly "the leading and most widely read financial computer bulletin board in the United States, where members can post statements regarding stocks, investments and other financial matters." *Id.*
193. *Id.* at *2.
194. *Id.*
195. *Id.* at *3.
196. *Id.* at *4.
197. *Id.*
198. *Id.*
199. *Id.* at *3.
200. *Id.* at *7.
201. *Id.*

202. *Id.* at *5.

203. *Id.* at *6.

204. *Id.*

205. *Id.*

206. *Id.*

207. *Today's News: Update*, N.Y. L.J., Dec. 14, 1995, at 1.

208. 907 F. Supp. 1361 (N.D. Cal. 1995).

209. *Id.* at 1365-66.

210. *Id.* at 1366.

211. *Id.* at 1372.

212. *Id.* at 1368.

213. *Id.* at 1369.

214. See *infra* part IV.E.1.

215. 907 F. Supp. at 1370 n. 12.

216. *Id.* at 1374.

217. *Id.*

218. *Id.*

219. *Id.* at 1381.

220. *Id.* at 1379.

221. *Id.* at 1372, 1381.

222. *Id.* at 1375, 1382.

223. See generally Henry H. Perritt, Jr., *Introduction: Symposium: The Congress, The Courts and Computer Based Communications Networks: Answering Questions About Access and Content Control*, 38 VILL. L. REV. 319, 321, 337 (1993); Henry H. Perritt, Jr., *Tort Liability, the First Amendment, and Equal Access to Electronic Networks*, 5 HARV. J. L. & TECH. 65, 73, 95 (1992).

224. See Eric Schlachter, *Cyberspace, the Free Market and the Free Marketplace of Ideas: Recognizing Legal Differences in Computer Bulletin Board Functions*, 16 HASTINGS COMM. & ENT. L.J. 87, 100, 133 (1993).

225. *Id.* at 127-28. See also David J. Loundy, *E-Law 2.0: Computer Information Systems Law and System Operator Liability Revisited*, Sept. 30, 1994, available at "URL:gopher://infolib.murdoch.edu.au:70/00/.ftp/pub/subj/law/jnl/elaw/refereed/loundy.txt" and "URL:ftp://infolib.murdoch.edu.au/pub/subj/law/jnl/elaw/refereed/ loundy.txt" on the Internet.

226. A common carrier is one who undertakes the transfer of all persons or property from one place to another indifferently. 13 C.J.S. *Carriers* § 2 (1990). Although telegraph, telephone, radio and television companies frequently have been termed "common carriers," their obligations and liabilities cannot be measured by the same rules which are applicable to common carriers of goods. So, while such companies are liable for negligence in the performance of their public duties, they are not liable as insurers. 86 C.J.S. *Tel. & Tel., Radio & Television* § 7 (1954).

The common carriers referred to in this section are those employed for wire or radio communication. Comparison with other common carriers, such as public transportation, is clearly inapplicable in cyberspace. Such carriers' duty to their customers is directly related to the physical transport of goods or people from one place to another.

227. 47 U.S.C. § 202(a) (1991).

228. The Federal Communications Act defines as a common carrier "any person engaged . . . for hire, in interstate or foreign communication by wire or radio." 47 U.S.C. § 153(h) (1988). Furthermore,

[a] public utility under a duty to transmit messages is privileged to do so, even though it knows the message to be false and defamatory, unless (a) the sender of the message is not privileged to send it, and (b) the agent who transmits the message knows or has reason to know that the sender is not privileged to publish it.

229. STATEMENT (SECOND) OF TORTS § 612(2) (1977).

. See *National Ass'n of Reg. Util. Comm'rs v. FCC*, 525 F.2d 630, 640-41 (D.C. Cir.), *cert. denied*, 425 U.S. 992 (1976) (One criterion for common carrier status is nondiscriminatory service to the public.) This special standard of liability is applied to common carriers in exchange for imposing the statutory obligation to provide nondiscriminatory service.

230. See *supra* part III.C.1.

231. 18 U.S.C. §§ 2510-2521, 2701-2711 (1994); see *supra* part III.C.1.

232. 18 U.S.C. § 2511(1) (1994).

233. 18 U.S.C. § 2511(3)(a) (1994).

234. Should the role and status of the system operator change in order to obtain the protection enjoyed by common carriers? How should sysop's activity be regulated in exchange for protection? It seems that technological evolution and the extension of access to any person in control of a computer, a modem and a telephone line will eventually inspire some regulations.

235. America OnLine, Inc., while declaring that it does not screen messages as a matter of policy, nevertheless sets forth strict "rules of the road" for on-line conduct. Any unpermitted act results in termination of membership. AMERICA ONLINE, INC., RULES OF THE ROAD §§ 2(C), (D), (E) (Apr. 10, 1996). The use of cryptography would make the sysop look more closely like a common carrier. Encryption, in fact, precludes sysops from reading the message and therefore tends to disprove their knowledge of the presence of harmful materials in their systems.

236. *Yugas v. Mudge*, 322 A.2d 824 (N.J. Super. Ct. App. Div. 1974). "To impose the suggested broad legal duty 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." *Id.* at 825.

237. See generally *Pittman v. Dow Jones & Co.*, 662 F. Supp. 921 (5th Cir. 1987) (action against newspaper after a Texas financial institution which advertised in it went bankrupt); *Winter v. G.P. Putnam's Sons*, 938 F.2d 1033 (9th Cir. 1991) (mushroom enthusiasts who became severely ill from picking and eating mushrooms sued the publisher of the book upon which they relied).

238. 968 F.2d 1110 (11th Cir. 1992), *cert. denied*, 506 U.S. 107 (1993).

239. The advertisement was the following: "GUN FOR HIRE: 37 year old professional mercenary desires jobs. Vietnam Veteran.

Discrete and very private. Body guard, courier and other special skills. All jobs considered . . ." *Id.* at 1112.

240. *Id.* at 1114.

241. *Id.* at 1117. *See also* Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'r of N.Y., 447 U.S. 557, 563-64 (1980).

242. The court reasoned that even though *New York Times v. Sullivan*, 376 U.S. 254, 279-80 (1964), had held that First Amendment protection "prohibits a public official from recovering damages for a defamatory falsehood relating to his official conduct unless he proves that the statement was made with 'actual malice,'" in subsequent opinions, the Court had clearly stated that the First Amendment does not require this high level of protection for all speech in all contexts. "In *Gertz*, for example, the Court held that a state could impose liability on a publisher who negligently printed a defamatory statement whose substance made 'substantial danger to reputation apparent.'" *Braun*, 968 F.2d at 1119 (citing from *Gertz*, 418 U.S. 323, 348 (1974)).

243. *Braun*, 968 F.2d at 1118.

244. The court distinguished *Eimann v. Soldier of Fortune Magazine, Inc.*, 880 F.2d 830 (5th Cir. 1989), *cert. denied*, 493 U.S. 1024 (1990), where the court had concluded that the standard imposed on the publisher by the Texas district court (a standard similar to Georgia's) was too high and would require a publisher to reject all ambiguous advertisements. *Braun*, 968 F.2d at 1115. In this case, the *Braun* court argued, the jury was correctly instructed that only an advertisement that contained a clearly identifiable unreasonable risk of harm to the public could impose liability on the magazine. *Id.* at 1116. The *Braun* court held that the advertisement in that case clearly conveyed that the advertiser was ready, willing and able to use his gun to commit crimes, and that language should have alerted a reasonable publisher to the risk. *Id.* at 1116 n.3.

245. *Id.* at 1115. The test follows Judge L. Hand's famous decision in *United States v. Carroll Towing Co.*, 159 F.2d 169, 173 (2d Cir. 1947).

246. *Braun*, 968 F.2d at 1115.

247. *Id.* at 1122.

248. How can the plaintiff show the degree of probability of harm? Past litigation in which the defendant sysop has been involved could be a good predictor of a higher degree of probability. This does not mean that plaintiff should prove that the sysop's activity or lack of security has a systemic positive impact on criminal acts. Certainly, however, the plaintiff would have to persuade the fact-finder that the probability of harmful activity, even if not systemic, is more likely than not.

Interestingly enough, *Soldier of Fortune Magazine, Inc.* has a long record of litigation for similar causes of action in other courts. *See, e.g., Eimann v. Soldier of Fortune Magazine, Inc.*, 880 F.2d 830 (5th Cir. 1989), *cert. denied*, 493 U.S. 1024 (1990) (refusing to declare the publisher liable for consequences that flow from his decision to publish any suspicious, ambiguous advertisement); *Norwood v. Soldier of Fortune Magazine, Inc.*, 651 F. Supp. 1397 (W.D. Ark. 1987) (noting that the publisher will be held liable if he publishes an advertisement that, to a reasonable person, indicates a substantial probability that will lead to harm).

249. Even the large sysop Prodigy has argued that the sheer volume of messages posted daily on its bulletin boards renders manual review an infeasible task. *See Stratton Oakmont, Inc. v. Prodigy*, NO. 31063/94, 1995 WL 323710, *3 (N.Y. Sup. Ct. May 24, 1995) (Stuart L. Ain, J.) (unpublished).

250. The strength of a similar test would probably be in the availability of statistical data related to the cost of adopting adequate precautions, the probability of harm and the gravity of the resulting injury. The proof of such statistical proxies probably would be an impossible effort for a nuclear entity like a small sysop, because of the cost of statistical analysis and the long-term pattern that any statistical study requires to be shown in order to be acceptable.

251. *See supra* part IV.B.

252. 50 AM. JUR. 2D, *Libel and Slander* § 369 (1995).

253. 361 U.S. 147 (1959).

254. *Id.* at 153 (footnotes and citations omitted).

255. *Id.* (quoting *The King v. Ewart*, 25 N. Z. L. R. 709, 729 (C. A.)).

256. *Id.* at 150, 160-61 (Frankfurter, J., concurring).

257. One commentator has proposed to hold a sysop liable in the same way private property owners can be liable for the defamatory statements of others if they control land or chattels and intentionally and unreasonably fail to remove defamatory matter that they know is exhibited. This suggests an analogy between the control that the sysop should have over its system and the control that the owner has over his private property. *See generally* Schlachter, *supra* note 224. However, the analogy is clearly faulty, since in modern times a private property's owner is regularly burdened by numerous duties that reduce his bundle of rights; these burdens are the result of general efficiency perspectives. To impose such burdens on a sysop would be equivalent to saying that the control owed by the sysop responds to a reason of efficiency, which is the exact opposite of our problem. Put in different terms, there can be no analogy because the property's owner is a beneficiary of a situation of power deriving from his property right, whereas the sysop is the provider of a service (the operation of the system).

258. *See* Becker, *supra* note 142, at 229. Prodigy prescreens all messages submitted for posting-over 100,000 weekly-in order to maintain its reputation as a "family service."

259. *See* *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135, 141 (S.D.N.Y. 1991).

260. *See* Becker, *supra* note 142, at 226-30.

261. 148 Mass. 513 (1889).

262. *Id.* at 515.

263. *Id.* at 516.

264. *Id.* at 518.

265. *Id.* at 517.

266. 244 P.2d 757 (Cal. Ct. App.1952).

267. *Id.* at 758.

268. *Id.* at 759.

269. *Id.* (footnotes and citations omitted). RESTATEMENT (SECOND) OF TORTS § 577 illus. 15 (1977) was derived from *Hellar. Tacket v. General Motors Corp.* 836 F.2d 1042, 1046 (7th Cir. 1987).

270. 259 N.E.2d 160 (Ohio Ct. App. 1970).

271. *Id.* at 161.

272. *Id.* at 162.

273. *Id.* at 161. The reasoning is contradictory and illogical. Indeed, a person might have a duty to prevent harm to the property of the plaintiff when there is a "special relationship" with the plaintiff or with the person who threatens the plaintiff. In the facts reported in *Scott*, the plaintiff and the owner of the building were under a special relationship, based upon the privity with the estate. The holding in *Scott*, by requiring a positive act by the owner of the building in order to assess his liability, overlooks all the aspects of the special relationship between persons in privity with the estate. In fact, in situations like landlord-tenant, hotel-guest, club-member and

university-student, the applicable rule is the negligence standard, which, in turn, expands the class of affirmative duties. *See* 57B AM. JUR. 2D *Negligence* §§ 1879, 1886, 1889, 1890, 1896 (1995). When one party submits himself to the protection and the control of the other, a duty is imposed upon the party who possesses control. For example, certain duties have been assigned to the landlord because of his *control* of common parts of the building; even though the landlord is not an insurer, he certainly is not a simple bystander. *See e.g.*, *Kline v. 1500 Mass. Ave. Apartment Corp.*, 439 F.2d 477 (D.C. Cir. 1970) (noting that a landlord controlling common areas has a duty to use ordinary care and diligence to maintain these areas in a reasonably safe condition).

274. *Hellar*, 244 P.2d at 758-59.

275. *Id.* at 759.

276. 836 F.2d 1042 (7th Cir. 1987).

277. *Id.* at 1047.

278. *Id.*

279. *Id.*

280. RESTATEMENT (SECOND) OF TORTS § 577(2) (1977).

281. *Id.*

282. *See supra* part IV.B.

283. *See supra* part IV.C.

284. *See supra* part IV.E.2.

285. Several commentators refer to this general purpose in their analyses. *See, e.g.*, Schlachter, *supra* note 224, at 124, 133-34; *See generally*, Loundy, *supra* note 225.

286. 361 U.S. 147 (1959).

287. 148 Mass. 513 (1889).

288. *See supra* part IV.E.3.

289. Most networks do not prescreen messages, but they will remove obscene or defamatory ones when other users complain. *See, e.g.*, AMERICA ONLINE INC., TERMS OF SERVICE AGREEMENT, ¶ 4(a) (effective date Dec. 5, 1995).

290. *See supra* part IV.E.4.

291. *Fogg v. Boston & L.R. Co.*, 148 Mass. 513, 517 (1889).

292. *Cf. id.* at 517-18.

293. *Cf. id.*

294. *Cf. id.*

295. The traditional rule of strict liability for abnormally dangerous activity does not seem to apply to system operators at all, not only because there is no *abnormal* risk involved in their activities, but also because they are likely to become of common valuable use for

the community. See RESTATEMENT (SECOND) OF TORTS, §§ 519, 520 (1977). An interesting but generally untapped approach would be to qualify the sysop's negligence within the modern theories of products liability.

296. See Schlachter, *supra* note 224, at 149-50. The author hints at this conclusion but does not develop it further.

297. International Soc'y for Krishna Consciousness v. Lee, 505 U.S. 672, 679 (1992); Cornelius v. NAACP Legal Defense & Educ. Fund, Inc., 473 U.S. 788, 800, 802 (1985). The first articulation of the public forum doctrine is contained in the famous statement by Justice Roberts:

Wherever the title of streets and parks may rest, they have immemorially been held in trust for the use of the public and, time out of mind, have been used for purpose of assembly, communicating thoughts between citizens and discussing public questions. Such use of the streets and public places has, from ancient times, been a part of the privileges, immunities, right and liberties of citizens.

298 *ague v. Committee for Industrial Organization*, 307 U.S. 496, 515 (1939).

. 424 U.S. 507 (1976).

299. *Id.* at 520 (emphasis omitted) (citing *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 210 (1975)).

300. 326 U.S. 501, 507 (1946) (setting aside the trespass conviction of a Jehovah's Witness who had distributed literature without a license on a sidewalk in Chickasaw, Ala, a so-called company town, wholly owned by the Gulf Shipbuilding Corp).

301. Edward J. Naughton, *Is Cyberspace a Public Forum? Computer Bulletin Boards, Free Speech, and State Action*, 81 GEO. L.J. 409 (1992).

302. See generally Schlachter, *supra* note 224.

303. See Daniel A. Farber, *Speech Without Romance: Public Choice and the First Amendment*, 105 HARV. L. REV. 554 (1991).

304. Public goods are goods for which "the benefits cannot be restricted to direct purchasers but inevitably spread to larger groups." Examples of public goods include clean air, national defense and information. Farber, *supra* note 303, at 558. On the Internet, once information is produced, it can be instantaneously reproduced and sent to a large number of individuals. The marginal cost of this is very little.

305. Farber, *supra* note 303, at 555 (emphasis omitted).

306. *Id.*

307. *Id.*

308. *Id.* at 556. "The First Amendment protection is based on the belief that people will make better decisions if they are more fully informed." *Id.* at 557-58. The economic model resembles traditional First Amendment doctrines because it is founded on the premise that people are rational individuals who can identify their interests and the means necessary for satisfying them. The similarity between the views of human nature underlying economic theory and the First Amendment make economics applicable to First Amendment doctrine. *Id.*

309. *Id.* at 559. The author concludes that "legal restrictions on information only further reduce a naturally inadequate supply of information." *Id.*

310. *Id.* at 559 n. 22.

311. Compare the suggestion proposed in the text with Farber, *supra* note 303, at 568-69. Nevertheless, such protections might cause the opposite effect of underdeterrence. Sysops could use their shield from liability to load questionable messages, articles and activities, which not only impose costs on privacy, but also considerable third-party costs. If the *New York Times v. Sullivan* test is

justified by the need to encourage free and robust debate, it nevertheless stirs various concerns. *See, e.g.*, Richard Epstein, *Was New York Times v. Sullivan Wrong?*, 53 U. CHI. L. REV. 782, 799-800 (1986). In an absolutely free environment, the honest and reputable people participating in public debate would bear the high cost of the *New York Times* standard. Rather than having to pay that cost with their reputation, these people may prefer to stay out of the public debate. *Id.* at 799. In an electronic environment, the effect may be to deter responsible people from using computer networks. Moreover, "[t]he level of discourse over public issues is not simply a function of the total amount of speech. It also depends on the quality of the speech." *Id.* at 799-800. If responsible people are overdeterred, information on computer network may be debased by its objectionable quality and content.

312. *See Schlachter, supra* note 224, at 212. The author notes that other characteristics which become irrelevant to group interaction include race, religion, sex, age, educational status and socioeconomic status, so that people are judged on the content of what they say.

Another author indicates that with "no national boundaries, physical obstacles such as oceans and deserts that have historically compartmentalized people are non-existent . . . [I]ndividuals are free to associate with others of their choosing . . ." Terri A. Cutrera, Note, *The Constitution in Cyberspace: The Fundamental Rights of Computer Users*, 60 UMKC L. REV. 139, 139 (1991).

313. Professor Burt Neuborne's contribution at the recent panel on *A Road Map on the Information Superhighway*, Vanderbilt Hall, New York University, April 29, 1995, suggested the same conclusion.

314. If we allow the state to regulate fraud and deceit in the economic marketplace, why not also in the marketplace of ideas? Why not allow the state to ban socially dangerous or coercive ideas, like racism and genocide, if we allow the state to ban dangerous consumer products in the economic marketplace? An eminent, Nobel Prize-winning economist has observed that the First Amendment seems to embody a laissez-faire approach to the market for ideas that the United States long ago abandoned in the market of goods. He suggests that since intellectuals trade ideas but not goods, they tend to oppose state regulation of ideas but favor regulation of goods. R. H. Coase, *The Market for Goods and the Market for Ideas*, 64 AM. ECON. REV. 384 (1974).

315. *Abrams v. United States*, 250 U.S. 616, 630 (1919).