The Law and the Internet

Daniel L. Appelman <dan@hewm.com>

Abstract

The increasing use of the Internet raises questions about the application of the law to communication in cyberspace. This paper examines two important areas of American jurisprudence, the laws of privacy and defamation, and suggests ways in which prior legal teachings might apply to the new medium.

1 Privacy

1.1 Constitutional Safeguards

Under the Fourth Amendment to the United States Constitution, any government action which violates a "reasonable expectation of privacy" constitutes a search. For searches to be valid, the state must obtain a warrant or an exception to the warrant requirement must apply. However, an individual does not have a "reasonable expectation of privacy" if he or she does not attempt to keep his or her communications private, for example, making statements where other persons may overhear. Additionally, an individual assumes the risk that any person with whom he or she communicates is "unreliable" and may either consent to government monitoring of a conversation or divulge information to the government.

The Katz and White cases both involve allegations that government law enforcement officials violated constitutionally- guaranteed rights of privacy in gathering information through electronic means. In the Katz case, the Supreme Court found a reasonable expectation of privacy when Katz was overheard by wire tap while talking in a public telephone booth. In the White case, the Supreme Court found no reasonable expectation of privacy when an informant secretly taped White's conversation in his house.

Two kinds of communication appear to be relevant to any discussion of privacy on the Internet. Those who post messages to and from USENET or other electronic bulletin boards can be assumed to have no reasonable expectation of privacy, since those bulletin boards are largely publicly available. It is less easy to determine whether a reasonable expectation of privacy exists or should exist among those who communicate by electronic mail. Do those who so communicate expect the same privacy as when they talk on the telephone? Is there something about the use of the Internet that makes it less secure and would justify a finding that no reasonable expectation of privacy exists unless, for example, the communicators encrypted their conversations? There are no cases which would give us further guidance on this matter. What is clear, however, is that encrypted communications have a greater expectation of privacy than non- encrypted communications do and that anything correspondence can do to enhance the confidentiality of their communications will be helpful in showing a reasonable expectation of privacy.

1.2 Electronic Communications Privacy, Act of 1986 ("ECPA")

The Fourth Amendment protects the privacy rights of individuals against action by governmental officials, not private individuals. The Electronic Communications Privacy Act, however, does provide for civil actions when the privacy rights of an individual have been breached by another individual.

1.2.1 Scope

The purpose of the ECPA is to regulate the nonconsensual interception and disclosure of wire, oral and electronic communications. "Electronic communications" are defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce" and, therefore, would include electronic mail and bulletin board messages. "Intercept" is defined as the "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." It therefore seems that the electronic communications which occur on the Internet are within the purview of the ECPA. Unlike the constitutional safeguards discussed above, the ECPA applies to individuals, partnerships, associations, joint stock companies, trusts and corporations as well as to government agents (so a finding of state action is not required).

1.2.2 Proscribed Activities

The ECPA prohibits the intentional interception, procurement, use or disclosure of any wire,

oral or electronic communication unless an authorization for interception has been obtained or one of several "exceptions" carved out in the act applies. One such "exception" seems to apply in the Internet context; this section of the act provides that "[i]t shall not be unlawful . . . for any person to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public." This "exception" seems applicable to the Internet environment because by virtue of the nature of the Internet, communications thereon, and especially bulletin board messages, are "readily accessible to the general public." Therefore, such communications may be intercepted without violating the ECPA.

1.2.3 Who is Liable?

From the language of the ECPA, it appears that only persons engaging in unauthorized interception and disclosure may be held liable, and that electronic communications service providers would not be held vicariously liable for such acts. In fact, one "exception" in the act states that "providers of wire or electronic communication service [and their employees and agents] are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in Section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider . . . has been provided with" a court order directing such action or certification of an authorized person that no warrant or court order is required, that all statutory requirements have been met, and that the provider's specified assistance is required.

Another such exception provides that "[a] person or entity providing electronic communications service to the public may divulge the contents of any such communication which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency."

Another, seemingly broad "exception" which is available to electronic communications service providers provides that:

It shall not be unlawful under this chapter for an. . . officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service . . . At least one commentator believes that this "normal course of business exception" allows for certain employers to monitor electronic communications of their employees.

Accordingly, it appears that the ECPA gives providers of electronic communications services a certain amount of flexibility with respect to interception and disclosure of electronic communications.

1.2.4 Criminal Penalties

Under the ECPA, any person who engages in interception and disclosure proscribed by the act is subject to criminal fines and imprisonment for up to five years.

1.2.5 Civil Causes of Action

There is some indication that the ECPA may "have some limited application to interception of data transmissions and electronic mail by private parties." [need to add more info after review house report] The ECPA specifically authorizes civil suits, preliminary injunctions and recovery of damages in civil actions. Civil damages awarded under the ECPA are assessed based on the greater of either (1) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, or (2) statutory damages of whichever is the greater of $100 a day for each day of violation or 10,000$. In addition, punitive damages may be assessed, and reasonable attorney's fees and costs may be awarded to a plaintiff.

1.2.6 Exclusionary Rule

Furthermore, the ECPA contains an expansive exclusionary rule which prohibits the use "in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof" if the disclosure of the intercepted information would contravene the act.

1.3 Privacy in the Workplace

A related issue is whether an employer can monitor an employee's electronic mail messages. A recent survey indicated that more than 20% of the businesses surveyed have searched computer files, voice mail messages, electronic mail messages and other communications of their employees. Thirty percent of companies with more than 1,000 employees have conducted such searches. The director of the American Civil Liberties

Union ("ACLU") National Task Force on Civil Liberties in the Workplace, Lewis Maltby, has indicated that violations of privacy in the workplace is the largest category of complaints received by the ACLU annually.

Courts which have considered this issue have generally held that employees do not have a reasonable expectation of privacy in electronic mail messages that they send via a system provided by the employer, and that the employer has the right to read any messages posted on such a system.

However, federal legislation has been introduced which would change this practice. The Privacy for Consumers and Workers Act ("PCWA") and other similar legislation would require employers to give employees advance notice of monitoring, and would limit the amount of monitoring an employer could do. Secret monitoring would be allowed only when the employer "has a reasonable suspicion that an employee is engaging in illegal activity or in conduct adverse to the employer's interests." Thus, employees would have more privacy in the workplace than they do now if PCWA or similar legislation is ever enacted into law.

2 Network Service Provider Liability for Defamation

One of the most pressing legal questions which has resulted from the increased use of computer bulletin boards is whether a computer service bureau should be held liable for defamatory messages published on a computer bulletin board by a subscriber. Since the Supreme Court has not yet decided a case involving computer bulletin board technology, the question must be answered by looking to the standards of liability that have been applied to other communication technologies and attempting to make the right analogies.

2.1 Computer Bulletin Boards and Current Libel Law

2.1.1 Electronic Publishing and Bulletin Boards

The computer bulletin board is a two-way computer communication service. Access to the service is acquired by purchasing a subscription from the owner of a large computer capable of bringing together many subscribers. Some bulletin boards accessible from the Internet are free. The subscriber is able to communicate inexpensively and instantaneously with a number of other users. Most bulletin boards are generally confined to a single topic of common interest. The types of speech encouraged and types of information provided by computer service bureaus are eclectic, ranging from personal and educational, to commercial and political. Some computer service bureaus, such as Prodigy, consider themselves responsible for all messages on the system, screening material and deleting obscene messages as well as those judged to be in poor taste. Other national computer service bureaus, such as CompuServe, do not assume responsibility for screening messages or monitoring communications among subscribers with any regularity, although they may in some instances where problems have come to their attention regulate problem users.

Many of the functions of a computer bulletin board are controlled by software. However, the bulletin board will still need to be overseen by a system operator ("SYSOP"). A SYSOP manages the large central computer through which subscribers send messages to each other and may exercise format or content control over messages disseminated by the bulletin board. A SYSOP does not ordinarily exercise format or content control until after a message is transmitted from one subscriber's terminal to the terminals of other subscribers. When a SYSOP observes a statement that is judged to be offensive or inappropriate for the board, the SYSOP is ordinarily authorized to remove that statement from all terminals on the board. However, since instantaneous transmission is an essential attribute of the electronic bulletin board, messages are generally not deleted until after they have already been sent.

2.1.2 Standards of Liability for Libel Vary According to the Type of Media Used for Publication

Libel is the publication of a false, defamatory and unprivileged statement to a third person by written or printed words or any other form of communication that has the potential harmful qualities characteristic of written or printed words. Current standards of liability for parties publishing libelous communications are a matter of common law to be decided by the states. The United States Supreme Court has established some minimum constitutional standards. In actions brought by private persons against media defendants, a negligence standard is applied with respect to truth or falsity and the publication must be intentional. In actions brought by public officials and public figures against media defendants involving libelous statements on matters of legitimate public interest, the libelous statement must be made either knowingly or with reckless disregard for the truth. In any action brought against a nonmedia defendant, there is no liability if a defendant did not intend to communicate

or publish a statement to a third person, attach a defamatory meaning to the statement, make the statement about the plaintiff, or communicate an untrue statement.

Reliable case law exists that applies the minimum constitutional standards of liability for libel to the print and broadcast media, common carriers, and traditional community bulletin board owners. It is possible to make analogies between these groups and the electronic communications provided by the Internet and electronic bulletin boards. From those analogies, a likely liability standard for libel for network service providers may be developed.

1. Broadcast and Print Media. In New York Times v. Sullivan, the Supreme Court recognized a national commitment to uninhibited, robust and wide open debate on public issues as well as a specific interest in preventing self-censorship by the press. The Court raised the standard of liability in cases brought by public officials against media defendants to "actual malice." A public official cannot recover in libel for a defamatory statement made by a media defendant unless he proves that the defendant acted with knowledge of falsity or reckless disregard for the truth in publishing the statement. Curtis Publishing Co. v. Butts, and Associated Press v. Walker, and Gertz v. Robert Welch, Inc., extended the actual malice standard to public figures and private individuals alleging libel by media defendants on a matter of public interest. The Supreme Court has not yet extended this broad First Amendment protection to defendants who are not members of any print or broadcast media.

   It is not clear whether network service providers on the Internet might be considered broadcast media. There is evidence that the Supreme Court might want to extend First Amendment protection to avoid the same chilling effect on free speech that it mentioned in the Sullivan case. In Dun & Bradstreet v. Greenmoss Builders, Inc., the Supreme Court considered for the first time whether the actual malice standard might apply if a defamatory communication was disseminated by a computer service bureau, in this case a credit reporting company that disseminated credit information by computer. The company disseminated a defamatory credit report to a small group of paid subscribers. In a plurality opinion, the Court ignored the lower court's conclusion that a credit bureau does not qualify as an organ of the media. Instead, the Court denied First Amendment protection to the computer service bureau on the ground that the message it reported was one of purely private concern.

   Justice Brennan wrote a dissent joined by three other justices which argued both that the media/non-media distinction is no longer relevant and further that even if the matter was only of private concern, it still should be protected against presumed and punitive damages under the Gertz standard. The plurality opinion written by Justice Powell declined to consider whether credit reporting agencies are, in fact, members of the media. Justice White wrote a concurring opinion in which he agreed with the dissenters that the media/non-media distinction was irrelevant but joined with the plurality in holding that First Amendment protection should be denied because the matter was of purely private concern.

   Five members of the Court, including Justice White in his concurrence and the four dissenters argued that the distinction between media and nonmedia defendants is no longer relevant. Justice Brennan observed that "owing to transformations in the technological and economic structure of the communications industry, there has been an increasing convergence of what might be labeled media and nonmedia." Thus, in Dun & Bradstreet, four members of the Court did not consider whether the computer service bureau was part of the media and five members of the Court felt that the Gertz standard should apply whether or not the computer service bureau was considered media.

   It appears then that the media/nonmedia distinction is probably no longer a factor in determining the level of First Amendment protection to be given to statements on computer bulletin boards. However, computer bulletin boards may still fail the matter of public interest requirement on a case-by-case basis. Thus, some communications on the bulletin boards, considered private communication, may be held to a lower standard of fault depending on the applicable state law, while other information on the computer bulletin board, considered matters of public interest, will be judged by the higher standard of liability under Gertz. This would require different treatment for different bulletin boards or even for different uses of the same bulletin board.

Analyzing the standard of liability for libel under Gertz depends on whether the information communicated is a matter of public concern. Dun & Bradstreet points otherwise, but the libel standard still might depend on whether the bulletin board is considered part of the media. If the matter is of public concern and the media distinction is irrelevant, then the bulletin board service provider will not be liable for libel unless the provider publishes statements with knowledge of falsity or reckless disregard. Given the volume of messages posted on bulletin boards and the impracticality of monitoring them all before posting, this standard would seem to shield network service providers and bulletin board providers from liability for libelous messages sent through their networks or posted on their computers.

2. Common Carriers. Under the Communications Act of 1934, "any person engaged as a common carrier for hire in interstate or foreign communications by wire or radio" is a common carrier subject to regulation by the F.C.C. More recently, the Supreme Court defined a common carrier as an individual or organization that offers a service to the public for hire, provides facilities to those who chose to purchase services to transmit messages created by the sender, and provides its services to the public without discriminating among members of the public. National Ass'n of Regulatory Utility Commissioners v. F.C.C..

   With respect to libel, common carriers have been considered secondary publishers because they ordinarily act only as conduits for transmission or carriage of a message created by the sender. Thus, common carriers have generally enjoyed immunity from liability as republishers. The rationale behind this immunity is based on notions of fairness and efficiency. Common carriers have little discretion to alter the messages they carry or prevent harm. Burdening common carriers with this responsibility would impair efficiency and violate the privacy of the public. However, if a common carrier has knowledge of the false and defamatory character of a message it has been hired to transmit or carry, and can prevent the harm, the common carrier bears a responsibility for the transmission. Common carriers are thus held to a knowing standard; they are subject to liability only if they know or have reason to know of a defamatory character of a message. In Western Union Telegraph Co. v. Lesesne, a federal court held that a telegraph company would be liable if an employee knew or had reason to know that the sender was not privileged to send the defamatory message.

   The analogy between computer bulletin board communication and common carriers is clear. The purpose of computer bulletin board communication is to facilitate rapid, spontaneous and economical transmission of matters of both private and public concern. This is the same purpose that the telephone, telegraph, microwave, satellite and mail services have. One difference is that the sender's privacy expectation in a computer bulletin board message sent to all bulletin board members must be less than the privacy expectation which attaches to communications with one person or a small group over a private telephone line. Another difference is that, although a computer service bureau system operator ordinarily does not view messages published until they have already been republished by the bulletin board, it is technologically possible for the messages to be checked. Checking a large volume of messages, however, would be economically impractical. Although the expectation of privacy is less in the case of a bulletin board user, it does seem that the actual knowledge standard as applied to common carriers would make the most sense as the standard for liability of the network service providers.

   The actual knowledge standard, or some variation of the actual knowledge standard, is probably the standard to which network service providers will be held. This may, in some instances, present the odd dilemma that a service provider is actually better off not knowing anything about the communications carried by it than it would be if the service provider did some selective monitoring and control. Thus, network service providers should be careful not to institute any program that would raise them to the actual knowledge standard without ensuring that whatever libelous messages were detected would immediately be removed from the system.

3. Traditional Bulletin Boards. Looking at cases involving traditional community bulletin boards helps to clear up the question of whether removing notices after they have been posted is sufficient to prevent bulletin board and network service providers from being liable. Hellar v. Bianco, held

> that once the proprietor or controller of a premises has noticed that defamatory material is present in the facility, failure to remove the defamation within a reasonable period of time will constitute a republication for which the proprietor or controller can be held liable. Under this analysis, republication does not occur when the notice is posted, but only after the notice has been allowed to remain up for longer than a reasonable time after the proprietor or controller of the bulletin board has notice of it.

This particular holding protects network service providers in two key ways. First, they do not often control any of the bulletin boards to which they will be providing their clients access. In this respect, they are more like common carriers such as the telephone company. They will have absolutely no control over what communication they relay. Second, as long as bulletin board operators are held to an actual knowledge standard, they will be safe from liability, to the extent that they do have any control over messages, as long they act promptly to remove any messages which become the subjects of complaints. This eliminates the problem of attempting to check messages before they are posted.

2.2 The Cubby, Inc. v. CompuServe, Inc. Case

The question of whether a network service provider would be liable for defamatory statements made on a bulletin board to which it provides its users access was considered in Cubby, Inc. v. CompuServe, Inc.. CompuServe provides computer related products and services, including the CompuServe information service, an on-line general information service for an electronic library that subscribers may access from a personal computer. Subscribers may obtain access to over 150 special interest forums which are comprised of electronic bulletin boards, interactive on-line conferences, and topical data bases. CompuServe contracted with Cameron Communications, Inc. ("CCI") 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. The district court found that CompuServe was not responsible for any libelous statements found on the bulletin board managed by CCI because it had neither knowledge nor reason to know of the allegedly defamatory statements.

The court acknowledged that one who repeats or otherwise publishes defamatory matter is subject to liability as if he had originally published it. The court then made the analogy to news vendors, book stores and libraries, stating that New York courts have long held that vendors and distributors of defamatory publications are not liable if they neither knew nor had reason to know of the defamation. In comparing CompuServe's provision of access to the bulletin board to the situation of a bookseller, the court noted that holding CompuServe liable would be like requiring every bookseller to make itself aware of the contents of every book in its shop. The court argued that it would be unreasonable to demand so near an approach to omniscience. The bookseller's burden would then become the public's burden because the public's access to reading matter would be restricted as a result of such requirements. "If the contents of bookshops and periodical stands were restricted to material which the proprietors has inspected, they might be depleted indeed."

The court noted that CompuServe uploads the data it receives and makes it available to subscribers almost instantaneously, and concluded that CompuServe's product is in essence an electronic for-profit library. CompuServe has no more editorial control over such a publication than does a public library, bookstore or newsstand. The court held that it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so. "First Amendment guarantees have long been recognized as protecting distributors of publications. Obviously, the national distributor of hundreds of periodicals has no duty to monitor each issue of every periodical it distributes." The court concluded that a computerized data base is the functional equivalent of a more traditional news vendor and the inconsistent application of a lower standard of liability to an electronic news distributor, such as CompuServe, than that which is applied to a public library, bookstore or newsstand, would impose an undue burden on the free flow of information. "The appropriate standard of liability to be applied to CompuServe is whether it knew or had reason to know of allegedly defamatory statements."

It is clear under the CompuServe case that providers of connections into bulletin boards would be safe from liability as long as they have no knowledge nor reason to know of defamatory statements on the bulletin board. What the case does not address is what the responsibility of a network service provider would be once it determined that a bulletin board to which it provides access contains defamatory material. In the CompuServe case, CompuServe retains some right to

edit the information on the bulletin board. A network service provider might not have the ability to edit any of the bulletin boards to which it provides access and could only prevent access to libelous material on the boards by canceling access to the entire bulletin board. A network service provider might still not be liable for any defamatory material it knows about because it cannot exercise any control over the board. However, courts might still hold network service providers liable because they could cancel the entire bulletin board connection.

2.3 Suggested Actions to Avoid Liability

Even though the final standard of liability for network service providers is not yet clear, there are steps which service providers may take which are likely to limit their liability.

1. Establish an identification code so that subscribers to the bulletin board are known to the operator by name and address. This would allow libelous messages to be traced and would enable the service provider to take action on any libel it notices.

2. Warn subscribers signing onto the service that (1) subscribers have a duty not to transmit libelous information, and (2) subscribers have a duty to notify the systems operator upon discovering any libelous transmission on a bulletin board.

3. Investigate and evaluate all reports of libelous messages on bulletin boards to which the service provider provides access.

4. Lodge complaints with bulletin boards which contain libelous information and consider terminating boards which continue to offend.

5. Remove subscribers who repeatedly post objectionable messages.

Adopting these measures industry-wide is important if the industry is to remain a self-policing one and not a heavily regulated industry.

A crucial determination for network service providers as opposed to bulletin board providers is the level of responsibility which a network service provider has for information on the computer bulletin boards which the network service provider knows is libelous but has no power to delete. At the present time, the only way to be certain to avoid liability is to drop the bulletin board. Network service providers also should note that, under the "know or has reason to know" standard, that when any knowledge of the information they are providing access to is gained or control is exercised, certain duties are triggered with respect to the service provider to prevent libel. The maxim that "a little knowledge is a dangerous thing" may very well apply in this case. A network provider may be safe if no monitoring of messages is done, or if full monitoring and removal of offending messages is instituted. The greatest danger would occur if limited monitoring occurs, and offending messages are noticed but not removed.