# Technology, Privacy, and Electronic Freedom of Speech

FRANCES M. McDONALD

## Introduction

DECISIONS BEING MADE NOW have the potential of creating a society in which all forms of communications are free or a society in which restrictions on access to information are imposed by legislators and other government officials. Unfortunately, based on precedents set with the regulation of radio and television, technologically uninformed government officials are passing laws without adequate attention to First Amendment freedoms and civil liberties.

> Electronic technology is conducive to freedom. The degree of diversity and plenitude of access that mature electronic technology allows far exceeds what is enjoyed today. Computerized information networks of the twenty-first century need not be any less free for all to use without let or hindrance than was the printing press. Only political errors might make them so.[1]

While technology has made it possible to access information at a rapid pace and in great diversity, current regulations impose a set of interlocking restrictions on that access to information. The morass of court decisions, Congressional legislation, and Federal Communications Commission (FCC) regulations which focus on technology ignore the Bill of Rights. First Amendment freedoms have not been applied to electronic distribution of information. Whether newspapers and other communications transmitted electronically will enjoy traditional press freedoms or be regulated as electronic broadcasting is still open to

Frances M. McDonald is Associate Professor, Library Media Education, and Coordinator, Technology in Education Program, Mankato State University, Mankato, Minnesota.

question. In addition to violating the First Amendment, recent technological advances have led to violations of the Fourth and Fifth Amendments. Using information stored in massive databases, the government, private industry, and individuals invade privacy with impunity.

In this article, five major issues related to the impact of technology on privacy and access to information will be explored. An overview of some of the abuses and the shortcomings of current attempts at regulating electronic communications will be provided.

1. *Regulation and licensing of the press.* The precedent of regulation of the press which began with the Radio Act of 1927 has resulted in almost unquestioned acceptance of regulating any forms of electronic communication today.
2. *Electronic surveillance.* Amassing information in huge computer databases leads to risks of massive governmental surveillance.
3. *Invasion of privacy.* Computers combined with a telecommunications link, provide virtually trackless access to any individual or organization wishing to peek.
4. *Copyright.* Copyright law, based on printed methods of communication, does not work when applied to the ownership of information existing only as electronic impulses.
5. *Policy-making and regulation.* The inability to anticipate the next technological advance leads to a patchwork of laws and regulations governing telecommunications and an incoherent national information policy.

The basis of American communication policy resides in the Constitution and the Bill of Rights.

1. Article I, Section 8 [8] gives Congress power to establish post offices and post roads. *(Common Carrier)*
2. Article I, Section 8 [8] gives Congress the power: "To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." *(Copyright)*
3. The First Amendment in the Bill of Rights prohibits Congress from passing any law abridging freedom of speech or of the press. *(Freedom of the Press)*

Competing with these rights are the protections provided in two other amendments in the Bill of Rights.

4. The Fourth Amendment provides: "The right of people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures." (*Privacy*)
5. The Fifth Amendment entitles all individuals to a range of procedural protections known as due process and states that "no person shall be compelled to be a witness against himself." (*Due Process*)

**Regulation and Licensing of the Press**

Eli Oboler[2] wrote that "the end of licensing of the Press was, of course, the beginning of true intellectual freedom in the United States." However, over the years, three communications models evolved without true intellectual freedom for all forms of communication: a print model free of regulation, a common carrier model with the government assuring nondiscriminatory access for all, and a broadcasting model with the government licensing owners as publishers.[3]

Each of the three models developed in a particular industry and for different types of communications. The press developed free of regulation. Based on concepts of monopoly, the common carrier approach evolved for telegraph and telephone. Then, based on concepts of spectrum scarcity and later on concepts of the public good, the broadcasting model evolved resulting in government regulation of radio and television. Since all media are now becoming electronic, "telecommunications policy is becoming communications policy."[4] Oboler asks in relation to the transformation of print media to electronic media:

> Is the cause of intellectual freedom helped or hindered by the late twentieth-century developments on many fronts of new ways to send, receive, store, and disseminate widely the vast amounts of information now available? Will the censor find new methods for censoring the vital communications so necessary to progress?[5]

Electronic media have never had the eighteenth- and nineteenth-century constitutional protections of no licenses, no special taxes, no regulations, no laws, and no prior restraint. Moreover,

> when wires, radio waves, satellites and computers became major vehicles of discourse, regulation seemed to be a technical necessity. And so, as speech increasingly flows over those electronic media, the five-century growth of an unabridged right of citizens to speak without controls may be endangered.[6]

The questions are: whether information policy will develop under the public interest, good-of-society regulations which now affect broadcast media; whether market conditions and property rights will be

allowed to dominate the development of telecommunications policy; whether the common carrier concept will be applied; or whether First Amendment freedoms will prevail in electronic communications. Currently, the government seems to favor diversity as deregulation breaks up communications monopolies. But, deregulation leading to a lifting of restrictions on press freedom appears unlikely.

When regulation began, the government viewed the telegraph as a business machine (like the computer later) and the issue of free speech did not arise. The high cost of sending a few words appeared to preclude the use of telegraphy for debate and expression. The courts concluded that the government had the authority to regulate telegraphy under commerce. Later, as newspapers began to use telegraph lines, the concept of news service developed. At first, carriers could choose not to carry news service traffic. But by 1893, the Supreme Court said telegraph was similar to common carriers requiring access without discrimination. Later, the common carrier concept was extended to telephone. While this appeared sensible since contact required individuals to be on the same line, it allowed a monopoly to develop.[7] As radio grew, the federal government required licenses to be issued in the public convenience, reasoning in terms of common carrier law. Today the same type of reasoning appears in telecommunications licensing.[8]

In 1920, the first radio station, KDKA Pittsburgh went on the air. Issues of scarcity, selective licensing, and free speech dominated the 1924 to 1927 debate leading to the Radio Act of 1927. Three points of view appeared in *The Nation.* David Sarnoff urged that the "same principles that apply to the freedom of the press should be made to apply to freedom of the air....The real danger is in censorship, in over-regulation."[9] Hudson Maxim wrote against free speech, although with some hesitation. "I distrust the wisdom of allowing radio broadcasting to be controlled by any private monopoly, but I also distrust the wisdom and the ability and the justice of federal control of radio....Perhaps the control of radio should be made quasi-private and quasi-governmental."[10] In the same issue, Grover Whalen argued for government control.[11] The next year, H.V. Kaltenborn appeared to be favoring a common carrier approach when he predicted that since the government would limit the number of stations, government should compel those stations to sell air time to "all comers on equal terms."[12] Ernst, in 1926, recognized that from the beginning, radio was subject to censorship—by the stations, in the selection of what ideas were broadcast; and by the government, in selecting which groups would be granted licenses to operate stations.[13]

As early as 1925, broadcasters had urged because of scarcity that no more licenses be issued and a common carrier approach to radio be adopted. "Broadcasting is as much of a public service and convenience as the telephone, and ultimately must be subject to the same kind of regulation and control."[14] Over the years, distrust of big business entered into decisions about regulation. Fear of AT&T led to rejection of the alternative of property rights for the new industry and regulation through licensing developed. "Both the motive and the effect of the Radio Act were to install government controls at the ground floor of the new industry before a structure of private rights could develop."[15]

The debate resulted in regulations promulgated on the basis of early use with no awareness of future technological advances. Although uses changed and television broadcasting arrived, regulations did not adjust. The concept of scarcity prevailed and the concept of equal time was introduced. Regulation of content expanded when *Red Lion*[16] established the Fairness Doctrine. While proponents favor the apparent access the Fairness Doctrine promises, critics point out that in practice, access is not enhanced. "The irony of the Fairness Doctrine is that broadcasters can fulfill it by tucking away an interview on a contrary viewpoint somewhere in the schedule."[17] Through licensing, equal time provisions, and the Fairness Doctrine, the government administers the content of broadcasting.

**Cable TV and the End of Scarcity**

Even before the advent of cable television, scarcity as an argument for continued government regulation had become untenable. Tighter channel spacing and the allocation of new frequencies through compression and multiplexing had increased the number of available channels. With the introduction of improved receivers and advanced telecommunications technology, spectrum scarcity is no longer a reality. Enclosed carriers (cable), the potential of fiber optics, and satellite transmission further diminish the scarcity argument. In addition, electronic memory now allows messages stored on videotape and videodisc to be delivered when convenient.[18] However, regulation continues.

Regulation of cable television has been divided between local franchising authorities and the FCC. Until 1965, the FCC declined jurisdiction creating a favorable environment for the growth of cable, but in 1965, the FCC put a freeze on new subscribers and banned cable television systems in the 100 largest markets from importing "distant signals." No longer wanting to stop growth, the FCC adopted new rules in the early 1970s. These rules which supported cable television were not

pro-freedom for cable television. Cable television was regulated in four areas—(1) signal carriage; (2) required or permitted offerings; (3) technical standards; and (4) division of responsibility between state, federal, and local governments. Signal carriage and required or permitted offerings have First Amendment implications.[19]

Local regulations, in the form of franchising agreements, served to assure access to those who wanted it. Pool called the resistance of the cable industry to requirements for channel leasing "self-serving" and described the "temptation for the cable monopoly to stifle uses that do not interest it" as good reasons for city governments to require nondiscriminatory access as part of franchising agreements. If cable is operated like a common carrier system, all who desire access may have access. When a cable carrier operates as a publisher, the operator may institute restrictions on who uses the system. Separating a carrier from content is both economically unwise and wrong on First Amendment grounds.[20]

Hints of issues of current concern were raised in 1969 when the FCC applied the requirement of equal time to rival candidates if newspaper publishers delivered news over cable channels. The FCC said:

> We do not intend to apply these requirements to the distribution of printed newspapers to their subscribers by way of cable....We have no intention of regulating the print medium when it is distributed in facsimile by cable [but] we do hold that the publication of a newspaper by a party does not put it in a different position from other persons when it sponsors or arranges for presentation of a CATV origin which does not constitute the distribution of a newspaper.[21]

Until recently, cable has been viewed primarily as entertainment. Now, cable performs as a two-way delivery system for all types of electronic traffic—computer data, electronic mail, videotext, information bases, education, security monitoring, teleconferencing, news services, movies, money, meetings, scientific data, opinion polling, manuscripts, petitions, editorials.[22] Two-way interactive television, while appealing in its ability to provide a variety of services, also carries with it dramatic risks to individual freedom and privacy. Burnham identified concerns about personal and collective privacy, uses, and regulation. Personal privacy risks exist when records about banking transactions, stock purchases, shopping patterns, and even the film-viewing habits of individuals are readily available. The ability to define the habits and interests of targeted groups of people through research on individual purchases, viewing patterns, and other uses of interactive television raises the larger issue of collective privacy. When speech recognition becomes possible, the prospect of increased surveillance expands.[23]

The 1984 cable television bill, while setting minimal federal restrictions on the cable industry, gives the franchising authority the power to censor "obscene" programming and allows the cable operator to censor "nonobscene, sexually-oriented programs" if the franchiser thinks the program is in "conflict with community standards."[24] The legislation fails to provide adequate guarantees for freedom of communication for cable. Further, the bill "restricts the import of leased access by limiting its provisions to video programming, thereby excluding computer languages, videotext, and other important and growing areas of cable use."[25] "Cable porn" legislation recently introduced into Congress could severely restrict, by federal mandate, what cable broadcasters would be allowed to transmit.[26]

Ignorance of potential technological advances, distrust of big business, and attempts to deter the development of communications monopolies led to regulation of broadcast media. Regulatory policy rather than information needs determined telecommunications policy. Owen suggested two factors to account for the acceptance of regulation of electronic media.

> First is simple ignorance on the part of courts, commissions, and congressional committees of the economics and technology of broadcasting....The other factor is a certain psychological attitude toward the electronic media. Many people regard television as being too powerful and influential to be allowed freedom from government control.[27]

*Solutions*

Critics of the current method of regulating broadcast media have offered a variety of proposals. Owen and Brazelon suggested deregulating but charging stations a reasonable spectrum use tax for the right to distribute programs over airways.[28] Kelley and Donway recommended repeal of the Fairness Doctrine and other content regulation, a transfer of current licenses into property rights, and an end to restrictions on entry, ownership, and conduct of business.[29] Wicklein proposed a decentralized common carrier "backbone system" available to everyone on a nondiscriminatory basis with no surveillance and no monitoring.[30] Krasnow believes the public trustee approach is constitutionally suspect and characterizes the regulation/deregulation scenario as applied to broadcasting as "political maneuvering."[31] Irwin suggests the time has come to allow regulation to be done by state governments, not the FCC.[32]

Attempts by Congress to extend First Amendment freedoms to the electronic media have not succeeded because of intensive lobbying by

the industry, by the FCC, and by special interest groups. Persons on both sides of the debate over broadcast media and the First Amendment call themselves real protectors of the First Amendment. In 1978, Van Deerlin and Frey introduced legislation to replace the FCC with a Communications Regulatory Commission. This met with intense opposition from all segments of the industry, the FCC, and special-interest groups. After attempting to appease critics by writing and rewriting the proposed legislation, the issue faded by 1980.[33] In the early eighties, Senator Packwood tried unsuccessfully to introduce legislation leading to First Amendment protections for electronic media.[34]

**Surveillance/Privacy**

While the discussion of regulation/deregulation of electronic forms of communication goes on, the issue of the capability of using electronic forms of communication to monitor the activities of citizens also demands attention. Alan Westin, an expert in issues of surveillance and privacy, pointed out that: "When a powerful (and expensive) new technology such as computers and communication systems is developed, the questions of who will use this new power, for what ends, and under what constraints becomes (once the potential for the new technology is recognized) more a matter of social policy than of technological determinism."[35] The computer has allowed us to create a "dossier society" that invades our privacy and threatens civil rights. Discussion of the threats focuses on how to balance privacy and other social interests with the content and control of computerized databases.[36]

Surveillance is "the systematic collection and monitoring of personal information for purposes of social control."[37] The National Security Administration (NSA) has installed voice-recognition, word-spotting devices that look for key phrases on transatlantic phone conversations. Markoff characterized NSA surveillance as an "invisible electronic...net over the entire population." Congressional hearings conducted during the mid-1970s revealed that for decades NSA had been intercepting international telegrams originating in the United States, and later, all radio and telephone conversations linked to this country looking for name and address combinations and trigger words.[38]

The government does not limit surveillance to private citizens but also monitors government employees. Privacy issues occur when the government monitors employee telephone calls using computer software which will spot frequently called numbers, long calls, and calls placed at unusual times. Civil libertarians warn about the chilling effect

such monitoring could have on forms of expression and on government whistle blowers. The government considers such surveillance perfectly legitimate pointing out that collecting information does not violate privacy, only disseminating information to third parties does.[39]

Not everyone shares concerns about the uses of government databases. Society approves the use of databases to identify dangerous drivers or to track welfare cheaters. Establishing eligibility for insurance and federal programs, defining and documenting details to meet bureaucratic obligations, determining credit and passport eligibility are accepted everyday uses of bureaucratic databases. While people protest unfair surveillance of themselves, they condone surveillance of others for any purposes they support. However, Rule warns that "we can conceive of no form of personal information which might not, under certain conditions, come to serve the purposes of bureaucracies aiming at some form of social control—brutal or humane."[40]

*Computerized Criminal Records*

National computerized criminal records are readily available and represent one of the most threatening databases. The criteria and standards enforced by the various states do not provide uniform information. Further, being arrested does not mean having committed a crime. Employers use criminal records to screen applicants for federal employment, the military, workers for government contractors, federal banks, and anywhere licenses and permits are required for a job. In New York, the "use of criminal records by law-enforcement agencies has declined in recent years, while its use by private employers has gone up."[41] Florida opens its records to anyone who will pay the search fee. In California, criminal history records serve to keep people unemployed. In spite of the fact that inaccurate records exist, opening criminal records to the public is not likely to result in innocent individuals checking records since they would be highly unlikely to expect to find a record. Even those who have reason to check are not likely to do so. In California, with 3 million records, only three hundred to four hundred ask to see records each year, and of these, eighty find incorrect information and only forty are successful in forcing California to correct their records. So, one in four who check find discrepancies, and one in ten force the state to make a correction. Further, responses to an Office of Technology Assessment questionnaire indicated that four of five states never conducted audits of the quality of the records.[42]

*Privacy Rights*

The basic rights involved in access to database records are those of personal privacy, personal access, and public access.[43] The Privacy Protection Study Commission (PPSC) identified five competing societal values in formulating public policy to protect personal privacy: "(1) First Amendment interest, (2) freedom of information interests, (3)the societal interest in law enforcement, (4)cost, and (5) federal-state relations."[44] Three criteria have been developed to protect privacy: maintaining accurate, complete, up-to-date records subject to review; citizens knowing uses which can be revoked; and organizations only using data on a need-to-know principle to attain their goals.[45]

The discussion of privacy and collection of data has "shifted from one of debate over privacy protection to one of elimination of abusive practices."[46] Burnham suggested that the right to see and correct our own records is viewed as the "miracle cure for many of the abuses of the computer age."[47] In fact, most remedies do not address the issue of privacy or the threat of massive surveillance finding its way into law. Recognizing that "freezing and dismantling" the record collection is unlikely, Chaum proposed restructuring major systems that use detailed information in a way that requires less information or using cryptographic techniques to mask individual records.[48] The problem lies in attempts to implement privacy laws without identifying people. Another suggestion, the use of a unique, reliable, personal identification, has itself the potential of leading to the invasion of individual privacy.[49]

*Computer Matching*

*Computer matching* is a term that has been applied to a variety of computerized data processing activities where separate files are run through a computer with a program set to detect certain matches. Computer matching is currently "being used to detect fraud and abuse in government programs by linking together formerly independent databases."[50] Westin thinks that banning computer matching is impossible. He thinks that at this point all we can do is monitor the amount of use and build safeguards into matching systems.[51] While warning that computer matching systems carry the potential for privacy and due process abuses, the American Civil Liberties Union (ACLU) also suggests that it is unrealistic to expect the government or organizations not to use computer matching.[52] Burnham stated that "increased sharing of information by all agencies of government gradually may be undermining the constitutional theory of checks and balances."[53] Particularly alarming is the assumption of guilt implied by computer matching. We are

"moving from a system relying on voluntary compliance and an assumption that citizens obey the law, to the assumption that citizens cannot be trusted."[54]

The government interprets the use of computer matching for purposes such as detecting welfare fraud and tracking runaway fathers to enforce child support to be legitimate government uses and point out that computer matching encourages efficiency. But Burnham asks whether the system which is so efficient at tracking fathers might actually have headed off other reforms that might have "improved the stability of American families." Once the system is established, what is to prevent it from later being used for the surveillance of other groups who fall into disfavor? If computer matching is successfully used for one kind of debt relationship, how do we assure it will not be expanded to other debt relationships? In a system set up to track segments of the population, inaccuracies present an important hazard.[55] Finally, the ACLU points out the risk of computer matching becoming computer merging resulting in the establishment of a national database?[56]

General computer matching violates our guarantees against unreasonable search and seizure, due process, and the assumption of innocence until proven guilty. To minimize computer matching abuses, the ACLU advocates a procedure called "front-end verification" in which only applicants for government services or a suspect's files would be checked rather than the government conducting general sweeps of databases looking for matches. Additionally, safeguards could be built into the system requiring notice that files are subject to matching, requiring verification of all matches, and requiring a hearing before benefits are denied or terminated on the basis of a computer match. All files created by a match should be destroyed after the match, further reducing privacy risks.[57]

**Illegal Computer Access**

Once the record collection has been put into place, the question of unauthorized access arises. There are three issues of concern. First, privacy rights of electronic communications; second, illegal computer access; and third, federal regulation of data communications.[58] Privacy rights have been discussed earlier.

Well-publicized activities of computer hackers illustrate how lack of security has made any database—whether educational, medical, or governmental—vulnerable to invasion. Hackers have successfully entered computers at Sloan-Kettering, the Department of Defense, the

Florida Department of Education, and the Los Alamos National Laboratory in addition to routinely entering corporate databases. A nineteen-year-old physics major at UCLA was arrested for entering defense department computers.[59] A *Newsweek* reporter's credit file was opened and credit card records distributed in retaliation for a story about bulletin boards.[60] But hackers are not responsible for all illegal computer activity. The San Francisco public defender's office accused police of spying on clients' records kept in a shared computer.[61]

Credit records are among the least secure of the giant databases. Credit bureaus have a "waiver of the nation's privacy laws" and have information about us we would not allow the government or anyone else to keep.[62] A large credit firm was sued to force it to tighten security against illegal access to credit files which contain lists of credit cards, credit limits, amounts owed, social security numbers, and inquiries. The credit company charged that the responsibility for allowing illegal access belonged to careless user companies whose employees are lax in protecting access code numbers and passwords.[63]

Although hackers receive the most publicity, much illegal access involves persons employed by data processing or electronic information companies. A recent survey of members conducted by the Data Processing Management Association revealed that of the 21 percent who said their organizations were victims of computer abuses, only 2 percent reported that the abuses were committed by outsiders. A survey of 130 prosecutors by the National Center for Computer Crime also reported that most computer crime was perpetrated by insiders.[64]

The term *hacker,* when used by computer enthusiasts, refers to people "involved in a wide range of computer related activities." When used by persons alarmed about illegal computer access, the term refers to a "person who often attempts to gain unauthorized access to large systems by using his personal computer equipment."[65] After an arrest connected with his hacker activities, Bill "Cracker" Landreth provided this rationale for unauthorized "exploration" of computers: "We were explorers, not spies." Hackers defend their activities by pointing out that most of them abide by a code of ethics, do not erase or damage files, do not write ridiculous or obscene messages, do not identify others, do not seek publicity, and do not leave tracks. "To hackers, what is known as 'browsing' is a (usually) harmless, 'educational' pursuit."[66] Sherry Turkle described hackers as intelligent students, mostly male, in "a culture of loners." Turkle's investigations show that from the hacker viewpoint, there is nothing wrong with inspecting (without invitation) programs and data files and that using others' programs is not stealing.[67]

However, the bad image of the hacker and his activities leads to legislative action and the fear that FCC regulation will sharply curtail activities of computer enthusiasts while at the same time doing nothing to deter serious online crime. Publicity about hacker activities led to the passage of the nation's first computer crime law, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984. The law imposes penalities for "unauthorized intrusion into computers holding electronic funds or national security data" and government-owned computers. Although not likely to pass during the fall of 1985, a bill to extend protection to private computers has been introduced. Over thirty states have computer crime legislation already in place.[68]

**Computer Networks**

One development of electronic technology which promises to provide information and publishing access for a wide variety of individuals is the communications network. Ranging from small privately operated bulletin boards to giant information databases operated for profit, these networks offer a delivery system for all types of communication. Poetry, fiction, news commentary, and spiritual messages as well as databases are all available through electronic information networks. Bulletin boards have become little newspapers providing publishing outlets for minority points of view.[69]

With the development of communications networks have come abuses. Phone numbers and credit card numbers are routinely listed for sale on "private boards." Computer programs appear in listings and copies are sold illegally and transmitted electronically. A southern California bulletin board operator faces criminal charges because an AT&T number was found on his board. Messages related to child pornography have been disseminated on computer bulletin boards. These activities cause legislators to focus on abuses rather than on protecting the First Amendment rights of bulletin board users. A commonly proposed solution is the requirement that bulletin board operators monitor messages carried on their systems and delete offensive or illegal messages. In California, a bill has been introduced which would make the system operator (sysop) "legally responsible for anything left on his bulletin board." This approach puts the bulletin board operator in the dual role of police and censor. Further, the bulletin board operator risks having the system shut down if illegal activity is found on it. Reacting to flaws in current and pending legislation, a California lawmaker introduced a bill proposing an amendment to the California

Constitution which would insure the privacy of electronic communications and provide for electronic freedom of speech.[70]

## Electronic Mail

By the year 2000, two-thirds of the nation's mail will be handled electronically. Although the Postal Service insists that its electronic mail system, E-Com, is secure, electronic mail poses potentially serious problems of security and privacy. Electronic mail offers an attractive target to anyone seeking access to individual and corporate information. Intruders can intercept and alter electronic mail. Since electronic mail creates a centralized record of who writes what to whom, the database developed presents the potential for private and government surveillance. Law enforcement officials need a warrant to open standard first class mail. The same letter in electronic form must be made available to officers with a subpeona or on demand of lawful authority, a much weaker restriction.[71]

Legislation has been proposed to protect the privacy of users of electronic mail and "provide legal protection against unauthorized government or private interception of new electronic communications." Electronic mail gives government agencies and others the ability to compile profiles of a highly personal nature on any individual by scanning messages for names, addresses, and topics. Messages are most vulnerable to interception when being held for forwarding or recorded for backup and audit purposes.[72] Because of legal precedents holding that citizens have no privacy rights in records held by third parties, uncertainty surrounds the legal status of electronic mail databases.[73]

During the summer of 1985, the government learned that an individual accused of cocaine trafficking had been exchanging messages with potential buyers and sellers using the electronic mail service operated by The Source. The Source refused to release its files to law enforcement officers on the grounds that messages entrusted to it are not "under its legal control." Since the defendant decided to plead guilty, the issue never went to court and the questions of legal control of files and Fourth Amendment protections have not been decided. However, the U.S. Attorney General's office suggested that since there was no legal precedent in the case, The Source had no grounds for its refusal to reveal its files.[74] Hints that offensive messages had been deleted by CompuServe, another electronic service, resulted in a statement by a CompuServe official that "CompuServe will 'never' engage in such E-Mail censorship."[75]

At the present time there are both private and public electronic mail operations. Bailey suggested that the surveillance problem might be more manageable if the private sector rather than the government ran automated clearinghouses and facilities for sending mail electronically. "In our 10-year effort to get the fair information practice philosophy articulated, we have tended to overlook the extent to which institutional pluralism can be an important safeguard for personal privacy in our society."[76] The ACLU advocates legislation which "protects the privacy of new electronic communication without unintentionally stifling technical or social innovation or inhibiting the free flow of information."[77]

**Electronic Publishing**

Electronic publishing is an outgrowth of the computer database industry. The prospect of publishing on demand, enabling scholars to have access to important titles, is only one aspect of the appeal of electronic publishing. On-demand publishing also allows the construction of individual profiles of readers' interests for selective dissemination of information. The ability of computers to scan electronic manuscripts for bibliographic information creates immediate databases for researchers. The greatest benefit of electronic publishing is that virtually anyone will be able to publish at will. Finally, electronic publishing allows for lower production costs, fewer errors, formatting standards, speed of production, and submission by electronic mail.[78]

Pournelle predicts the establishment of an "Electronic Village" creating a synergistic effect on the generation of ideas. "When the Founding Fathers wrote freedom of the press into the Constitution, they intended to protect far more than big city newspapers; they also had in mind the smaller-scale activist pamphleteer. Thomas Paine's *Common Sense* was more in their minds than the London *Times*." While publishing a newspaper requires considerable money, a computer network is available to nearly everyone. Pournelle predicts that the ready availability of networks will make suppression of ideas almost impossible.[79]

Unanswered questions about the status of electronic publishing exist. Electronic publishing is a mix of long-term and local storage with telecommunications links delivering information to the user's premises. If electronic publishing is viewed as publishing, traditional press freedoms will apply. But, if electronic distribution of information over telephone lines on cable television is viewed as broadcasting, regulation could occur. "The cause for fear is that when its (electronic publishing or on-demand publishing) technology looks like that of an office the

law may see it as commerce, not publishing and thus subject to regulation like any business."[80]

As publishing increasingly becomes electronic, the risk of widening the gap between the information rich and information poor emerges as an issue of social concern. Unless individuals have free access to information regardless of format, those least likely to have access through their own personal computers will have no access at all. Institutions providing access to electronic databases now rarely provide the service without cost.

## Copyright

Authority to establish copyright law is embodied in the Constitution. If the concept of copyright is accepted as enhancing the free flow of ideas by stimulating creative work, one must live with the restrictions copyright puts on the use of another's intellectual property. The "laws of copyright are among the most obvious but least condemned restraints on freedom of expression."[81] Pool concluded that the idea of "the objective of copyright is beyond dispute. Intellectual effort needs compensation." But "to apply a print scheme of compensation to the fluid dialogue of interactive electronic publishing will not succeed."[82]

Copyright issues arise in the discussion of all forms of electronic communication. Computer programs generate abstracts and create databases. The programs are copyrightable, but questions exist about who owns the generated text. The "idea that a machine is capable of intellectual labor is beyond the scope of copyright statutes. Can a computer infringe copyright?"[83] Participants in computer conferencing sharing ideas with strangers risk having their individual ideas taken and used. Zientara reports that computer conferencing is largely based on trust and that electronic messages are implicitly copyrighted in the name of the person who inputs them but, if no notice is included, others can use the ideas. If "on-line conferences [are] regarded as databases with their own intrinsic value," who should hold the copyright?[84] Bibliographic control as we know it is also likely to change as the concept of uniform copies changes. As users modify and expand text, different versions will be stored in different locations. In the instance of full text databases, does storage on disk memory for later use violate copyright?[85]

### *Piracy of Software*

The area of copyright and technology receiving the most publicity is the piracy of computer software. The Software Publishers Association

(SPA) has had some success in stopping illegal copying of software primarily by personal contact, investigation, and threats of lawsuits. A threatened lawsuit against a school district in Ohio resulted in the school district's promise that policy guidelines would be adopted. Industry officials intend to continue such pressures to stem the tide of illegal copying. Pirate bulletin boards are monitored by the SPA to identify copyright violation for potential prosecution.[86]

Major corporations nationwide are also caught in the illegal software net. Apple computer officials, after conducting an investigation of employees within the company, concluded that employees "regularly distribute pirated software among themselves, as well as outside the company." Officials attributed the copying to "Apple's original 'hacker ethic.' " However, an Apple vice-president concluded that Apple's compliance with copyright and the law is 99 percent.[87] The success of a recent lawsuit against a national corporation by the software company Micropro is expected to have an impact on corporate piracy of software.[88]

*Licensing*

The software industry has instituted various methods to inhibit illegal copying. Copy protection devices and site licensing are two such attempts. However, questions have been raised about the legality of some of these methods. Licenses include restrictions that go beyond the copyright law. A computer law attorney stated that: "Most of the license forms I've seen fail to distinguish the intellectual property and physical property."[89] Software publishers interpret copyright law to mean that only the purchaser of a program has the right to use the program and then only in one location and on one machine. Strong consumer and legal objections are being heard about the application of copyright to microcomputer software. Software industry interpretations which dictate the users and uses of software and licensing are of special concern.[90]

Software producers offer site licensing as the solution for educational institutions and corporations which require several individuals to use the same program at the same time. Fawcette sees site licensing as an "umbrella to cover general dissatisfaction by corporate micro managers or information center managers with the policies of the software industry." Reflecting the users at large, Fawcette lists the concerns as copy protection, customer support, and network licenses which obstruct the ability to use software on networks.[91]

One of the most controversial of the attempts to limit copying has been the shrink-wrap license. Under a shrink-wrap agreement, the opening of the wrap is supposed to put a contract into effect. Experts

hold differing opinions about the legality of the concept of shrink wrap. Of concern to software users is the issue of being held accountable to a contract they had no hand in writing and might not be able to read clearly and understand. Louisiana passed specific legislation making computer software purchasers legally responsible for abiding by the shrink-wrap terms on the package. Louisiana's law is written so that no proof needs to be provided that users consented to the shrink-wrap agreement.[92] A lawsuit designed to test Louisiana's shrink-wrap law was recently dismissed by a district court judge in New Orleans.[93] The industry had anticipated that the decision in the Louisiana case would help to eliminate some of the confusions about the application of the law to microcomputer software.

Other measures have been proposed. One antipiracy scheme would license owners of computers with a unique identification code installed in the computer's hardware. Software writers would have to program traps in software to look for special serial numbers. Since both hardware and software purchases would be known and recorded for the scheme to work, the potential for violation of privacy as well as restraints on purchases exists. Another solution being proposed by the software industry is the attachment of special devices into the computer.[94] Not all software users find the use of such devices reasonable. The publisher of *InfoWorld* called the introduction of the key device "extremist" and found it unreasonable to use a special port to hook up a hardware key to prevent software copying.[95]

The Office of Technology Assessment recently released a study of new information technologies related to intellectual property rights and is expected to have a publication identifying problems, issues, and gaps in current law.[96]

## Conclusion

Certain principles must be applied to electronic forms of communications to insure that First Amendment freedoms, privacy, and access considerations are protected. The First Amendment must be applied fully to all media giving anyone—whether cable operator, major broadcast network, or computer networker—the opportunity to publish without licensing or scrutiny by the government. Prior restraint regulations must not be allowed to dominate electronic publishing. Privacy, due process, and protection from self-incrimination must be built into any regulatory scheme imposed on electronic communications. Copyright enforcement must be adapted to the new technology. "Control of the system, restrictions on freedom of expression, intrusions on privacy,

and threats to individual liberty" are issues which must be debated and policies developed at the national level.[97]

Electronic freedom of speech is as essential as print freedoms. Today's corner orator now finds an audience on an electronic bulletin board. The patchwork of existing and pending legislation, drafted in reaction to abuses of the moment, will not serve to build the coherent national policy needed for communication through electronics. At the present time, the FCC is experiencing serious problems trying to fit new technologies into its current regulatory scheme.[98] The "lack of technical grasp by policy makers and their propensity to solve problems of conflict, privacy, intellectual property, and monopoly by accustomed bureaucratic routines are the main reasons for concern."[99] Passing further piecemeal legislation and regulations must be halted until a coherent national information policy can be adopted. Unless this happens, erosion of First Amendment rights and civil liberties will continue.

## References

1. Pool, Ithiel de Sola. *Technologies of Freedom.* Cambridge: Belknap Press of Harvard University Press, 1983, p. 231.

2. Oboler, Eli M. *To Free the Mind: Libraries, Technology, and Intellectual Freedom.* Littleton, Colo.: Libraries Unlimited, 1983, p. 61.

3. Pool, *Technologies of Freedom,* p. 233.

4. Ibid.

5. Oboler, *To Free the Mind,* p. 5.

6. Pool, *Technologies of Freedom,* p. 1.

7. Ibid., pp. 91-96.

8. Ibid., p. 103.

9. Sarnoff, David. "Freedom of the Air: Uncensored and Uncontrolled." *The Nation* 119(23 July 1924):90.

10. Maxin, Hudson. "Freedom of the Air: Radio—The Fulcrum." *The Nation* 119(23 July 1924):91.

11. Whalen, Grover A. "Freedom of the Air: Radio Control." *The Nation* 119(23 July 1924):91.

12. Kaltenborn, H.V. "On Being 'On the Air': Behind the Footlights in a Broadcasting Studio." *The Independent* 114(23 May 1925):583-85.

13. Ernst, Morris L. "Who Shall Control the Air?" *The Nation* 122(21 April 1926):443-44.

14. Pool, *Technologies of Freedom,* p. 121.

15. Kelley, David, and Donway, Roger. *Laissez Parler: Freedom in the Electronic Media.* Bowling Green, Ohio: Bowling Green State University, Social Philosophy and Policy Center, 1983, p. 14.

16. *Red Lion Broadcasting Co.* v. *FCC* 89 S. Ct. 1794 (1969).

17. Small, William. "Radio and Television Treated Like Distant Cousins." In *The First Freedom Today: Critical Issues Relating to Censorship and to Intellectual Freedom,* edited by Robert B. Downs and Ralph E. McCoy, p. 319. Chicago: ALA, 1984.

18. Pool, *Technologies of Freedom,* p. 152.

19. Ibid., pp. 157-58; and Carter, T. Barton, et al. *The First Amendment and the Fourth Estate: The Law of Mass Media*, 3d ed. Mineola, N.Y.: The Foundation Press, 1985, pp. 642-57.

20. Pool, *Technologies of Freedom*, pp. 239-40.

21. Ibid., p. 159.

22. Ibid., pp. 167, 227.

23. Burnham, David. *The Rise of the Computer State: The Threat to Our Freedoms, Our Ethics and Our Democratic Process.* New York: Random House, 1983, pp. 242-49.

24. "Cable TV Bill Passes in Final Hour of 98th Congress." *Civil Liberties Alert* 8(Jan. 1985):6.

25. American Civil Liberties Union. "The ACLU and Cable Television: A Critique of the New Federal Legislation." Washington, D.C.: ACLU, 1984, p. 3 (pamphlet).

26. Lynn, Barry W. "Testimony Regarding Regulation of 'Cable Porn' and 'Dial-A-Porn.'" U.S. Senate. Judiciary Subcommittee on Crime, 31 July 1985. Washington, D.C.: ACLU, 1985.

27. Owen, Bruce M., and Bazelon, David L. "Different Media, Differing Treatment?" In *Free but Regulated: Conflicting Traditions in Media Law*, edited by Daniel L. Brenner and William L. Rivers, p. 44. Ames: Iowa State University Press, 1982.

28. Ibid., p. 63.

29. Kelley, and Donway, *Laissez Parler*, pp. 43-44.

30. Wicklein, John. *Electronic Nightmare: The New Communications and Freedom.* New York: Viking Press, 1981, pp. 249-53.

31. Krasnow, Erwin G., et al. *The Politics of Broadcast Regulation*, 3d ed. New York: St. Martin's Press, 1982, pp. 21, 27.

32. Irwin, Manley R. *Telecommunications America.* Westport, Conn.: Quorum Books, 1984, pp. 126-28.

33. Krasnow, *The Politics of Broadcast Regulation*, pp. 240-70.

34. U.S. Senate. Committee on Commerce, Science and Transportation. *News Release*, 97th Cong., 2d sess., 28 Sept. 1982.

35. Westin, Alan F. "The Long-Term Implications of Computers for Privacy and the Protection of Public Order." In *Computers and Privacy in the Next Decade*, edited by Lance J. Hoffman, p. 168. New York: Academic Press, 1980.

36. Ibid., pp. 167-81.

37. Rule, James B., et al. "Preserving Individual Autonomy in an Information Oriented Society." In *Computers and Privacy in the Next Decade*, p. 68.

38. Markoff, John, et al. "Federal Court Okays Sweeping Surveillance Privileges." *InfoWorld* 5(4 April 1983):14-15; and _____ . "Electronic Surveillance Menaces Personal Privacy." *InfoWorld* 5(11 April 1983):16-17.

39. Tucker, Elizabeth. "Would '1985' Have Been a Better Title for '1984'?" *Washington Post* (National Weekly edition), 25 March 1985, p. 28.

40. Rule, "Preserving Individual Autonomy," p. 71.

41. Burnham, *Rise of the Computer State*, p. 77.

42. Ibid., pp. 75-82.

43. Everest, Gordon C. "Nonuniform Privacy Laws: Implications and Attempts at Uniformity." In *Computers and Privacy in the Next Decade*, pp. 141-50.

44. Sitkin, Irwin J. "Comment on 'Privacy Cost Research: An Agenda.'" In *Computers and Privacy in the Next Decade*, pp. 61-64.

45. Rule, "Preserving Individual Autonomy," p. 74.

46. Ibid., p. 73.

47. Burnham, *Rise of the Computer State*, p. 81.

48. Swaine, Michael. "Taking a Pseudonym Can Prevent 'Dossier Society.'" *InfoWorld* 5(12 Sept. 1983):19.

49. Goldstein, Robert C. "Privacy Cost Research: An Agenda." In *Computers and Privacy*, pp. 51-56.

50. Berman, Jerry J., and Dame, Lauren. "ACLU Privacy and Technology Project." Washington, D.C.: ACLU, 1985, p. 2 (pamphlet).

51. Westin, "Long-Term Implications of Computers," p. 178.
52. Berman, and Dame, "ACLU Privacy and Technology Project," p. 3.
53. Burnham, *Rise of the Computer State,* p. 29.
54. Berman, and Dame, "ACLU Privacy and Technology Project," p. 13.
55. Burnham, *Rise of the Computer State,* pp. 29-33.
56. Berman, and Dame, "ACLU Privacy and Technology Project," p. 14.
57. Ibid., p. 12.
58. Meeks, Brock N. "Telelaw vs. Electronic Freedom of Speech." *LinkUp* 2(Sept. 1985):22-23.
59. Hafner, Katherine. "UCLA Student Penetrates DOD Network." *InfoWorld* 5(21 Nov. 1983):28; Shea, Tom. "The FBI Goes After Hackers." *InfoWorld* 6(26 March 1984):38-43; and "Student 'Hacker' Cracks Code, Enters Education Files." *Education Week* 5(9 Oct. 1985):3.
60. Watt, Peggy. "Hack Attack Alarms Hobbyists." *InfoWorld* 6(31 Dec. 1984):17.
61. Bannister, Hank. "Police Accused of Computer Spying." *InfoWorld* 7(18 March 1985):15-16.
62. Watt, "Hack Attack Alarms Hobbyists," p. 17.
63. _____. "Credit Bureau Sued on Security." *InfoWorld* 6(3 Dec. 1984):18.
64. Ranney, Elizabeth. "Data Security Violated Mostly on the Inside, 2 Studies Show." *InfoWorld* 7(23 Sept. 1985):1.
65. Landreth, Bill. *Out of the Inner Circle: A Hacker's Guide to Computer Security by "The Cracker": The Teenage Computer Wizard.* Bellevue, Wash.: Microsoft Press, 1985, p. 26.
66. Ibid., p. 207.
67. Turkle, Sherry. *The Second Self: Computers and the Human Spirit.* New York: Simon & Schuster, 1984, pp. 196-238.
68. Mace, Scott. "Computer Bills in Works." *InfoWorld* 7(14 Oct. 1985):10; Markoff, John. "Teen-hackers' Antics Prompt House Hearing." *InfoWorld* 5(7 Nov. 1983):26; and _____. "New Laws May Penalize Bulletin-Board Hackers." *InfoWorld* 5(21 Nov. 1983):27.
69. "Here Come the Networkers." *Newsweek* 126(25 Nov. 1985):100.
70. Meeks, "Telelaw vs. Electronic Freedom," p. 22.
71. Rosenfeld, Seth. "Who's Reading Your Electronic Mail?" *InfoWorld* 5(12 Dec. 1983):24-26.
72. Berman, Jerry J. "Testimony on S. 1667 The Electronic Communication Privacy Act of 1985." U.S. Senate, Senate Judiciary Committee, Subcommittee on Patents, Copyrights and Trademarks, 13 Nov. 1985. Washington, D.C.: ACLU, 1985 (pamphlet).
73. *United States* v. *Miller,* 425 U.S. 435 (1976).
74. Howitt, Doran. "Court Pries Into E-Mail." *InfoWorld* 7(15 July 1985):26.
75. Berstein, Paul, and Casman, Steve. "Who's Reading the Mail?" (letters section). *InfoWorld* 7(11 March 1985):6.
76. Bailey, Carole Parsons. "Comment on 'Privacy in Electronic Funds Transfer, Point of Sale, and Electronic Mail Systems in the Next Decade.'" In *Computers and Privacy in the Next Decade,* pp. 45-50.
77. Berman, "Testimony on S. 1667," p. 1.
78. Haas, Warren J. "Computing in Documentation and Scholarly Research." *Science* 215(12 Feb. 1982):857-61.
79. Pournelle, Jerry. "The Real Electronic Village." *Popular Computing* 4(Oct. 1985):45-49.
80. Pool, *Technologies of Freedom,* p. 194.
81. Carter, *The First Amendment,* p. 178.
82. Pool, *Technologies of Freedom,* p. 249.
83. Ibid., p. 215.
84. Zientara, Marguerite. "Watch Your Words: Who Owns Information in an Electronic Conference?" *InfoWorld* 6(6 Aug. 1984):33-34.
85. Pool, *Technologies of Freedom,* p. 213.

86. "School Districts Singled Out on Piracy Charges." *Classroom Computer Learning* 6(Oct. 1985):14.

87. McGeever, Christine. "Software Piracy Troubles Apple Officials." *InfoWorld* 7(2 Sept. 1985):1.

88. Chin, Kathy. "Conglomerate Sued for Piracy." *InfoWorld* 7(4 Feb. 1985):17.

89. _____ . "The Software License Quagmire: The Irony of Unenforceable Contracts." *InfoWorld* 6(25 June 1984):34-35.

90. Stein, Allan. "License to Own Computers—Projections of a Paranoid?" *InfoWorld* 5(3 Oct. 1983):37-38.

91. Fawcette, James E. "Site Licensing Crucial." *InfoWorld* 7(22 July 1985):5; Pournelle, Jerry. "Of Publishers and Pirates." *Popular Computing* 4(Dec. 1984):59-62; and Becker, Gary. "Software Copyright Looks Fuzzy, But Is It?" *Electronic Education* 4(Oct. 1984):18-19.

92. "'Shrink-Wrap' Law to Receive Its First Test." *TechTrends* 30(Sept. 1985):3; and Ranney, Elizabeth. "First Test for 'Shrink-Wrap' Law." *InfoWorld* 7(8 July 1985):22.

93. Ranney, Elizabeth. "State 'Shrink Wrap' Piracy Suit is Dismissed by Judge." *InfoWorld* 7(21 Oct. 1985):6.

94. Mace, Scott. "Devices Allow Backups Yet Inhibit Piracy of Programs." *InfoWorld* 7(16 Sept. 1985):15.

95. Fawcette, James E. "Fighting Common Sense." *InfoWorld* 7(4 March 1985):5.

96. "The New Agenda on Intellectual Property Rights." *TechTrends* 31(May/June 1986):3.

97. Wicklein, *Electronic Nightmare,* p. 242.

98. Carter, *The First Amendment,* p. 657.

99. Pool, *Technologies of Freedom,* p. 251.