July 1992 Vol. 4; Issue 5

ELECTRIFYING SPEECH

New Communications Technologies and Traditional Civil Liberties

Contents

INTRODUCTION: NEW COMMUNICATION TECHNOLOGIES

Since the personal computer ushered in a communication revolution about 15 years ago, the accompanying technology has been likened to everything from the printing press to Hyde Park Corner, from the postal system to talk radio. Pungent as these analogies are, their limitations point up the essential uniqueness of computer-mediated communication. While the printing press made possible the mass dissemination of information, computers can individualize information and increase its flow a thousandfold. In the process, they change the nature of communication itself.

Few Americans are unaffected by this revolution, whether they rely on computers to do their taxes, write a novel, serve up money from a bank machine, or make airplane reservations -- and then guide the plane safely back to land. Those who are "on-line" "talk" to people whom they may never meet face-to-face and form "virtual communities" in "Cyberspace" -- a place without physical dimensions, but with the capacity to store vast amounts of facts, conversation, messages, written or voice mail and graphic images.

While it is axiomatic that these new capabilities can open up faster, easier and more inclusive

communication, they also call into question long held assumptions about individual and communal rights. Some are old questions in a new context: What, if any, is the role of the government in regulating electronic communication? As more and more information is recorded and stored automatically, how can the right of privacy be balanced with the right to know? What happens to individual protections when information is a saleable commodity? Does the form in which information is kept change the government's obligation to inform its citizens?

Other questions arise from the new technologies: When borders can be breached by a keystroke and texts and images can be reproduced and modified without ever being published, what happens to definitions of intellectual property, scholarship, conversation, publication, community, even knowledge itself?

In 1983, Ithiel de Sola Pool began his seminal book, *Technologies of Freedom*, with the warning that "Civil liberty functions today in a changing technological context."[1] As if to prove him right, the government is now proposing a $2 billion investment in computer networking technologies which will radically alter the way American communicate. Because the technological context changes more rapidly than the laws regulating it, the debate about how we want to live in an electronic world is both volatile and urgent.

ELECTRONIC COMMUNICATION AND THE LAW

United States law has not treated all communication technology alike. As Pool notes, regulatory policy is based on different assumptions and varies among print, common carriage and broadcasting, which were the three prominent modes of mass communication when he wrote. Thus, lawmakers and jurists delineating free speech sought to minimize traditional controls on printed speech by rejecting the types of censorship associated with it, such as prior restraint, taxation and seditious libel. But early regulators, with an eye to the social good, had no qualms about requiring common carriers, such as the postal and telegraph systems, to provide universal service without discrimination. Their successors, assuming that the broadcast spectrum was a scarce commodity, designed a regulatory system for radio and TV based on government licensing, business advertising and a limited number of channels. Later regulations included the Fairness Doctrine (imposing on licensed broadcasters an obligation

[1] Pool, Ithiel de Sola, *Technologies of Freedom*, Cambridge, Mass.: Harvard University Press, 1983.

to cover issues fairly), which regulated the content of speech. But as technologies merge, traditional distinctions among the modes are no longer applicable. Today, for instance, anyone regulating electronic bulletin boards is looking at a cross between a publisher and a bookstore that operates by means of the telephone, a common carrier.

Historically, the law has responded to, not anticipated, technological changes, often reacting repressively when a new technology challenges the status quo. As in the past, regulation of electronic communication has been influenced more by market and political forces than constitutional principles or legal issues. But electronic communication policy is still fluid enough to allow for questions about who should set the policy and to what end.

The Constitution

Among the most active participants in the policy discussion is Computer Professionals for Social Responsibility (CPSR), a public interest group formed to explore the impact of computers on society. In March 1991, CPSR held the First Conference on Computers, Freedom & Privacy in Burlingame, California. The concerns addressed at the conference fell into three broad civil liberty categories: protecting speech, protecting privacy, and gaining access to government information.

In an opening address, constitutional scholar Laurence Tribe posed a question of his own: "When the lines along which our Constitution is drawn warp or vanish, what happens to the Constitution itself?"[2] The sections of the Constitution Tribe was referring to in relation to electronic communication are:

- the First Amendment, with its prohibition against laws abridging freedom of speech, assembly, or the press;
- the Fourth Amendment, protecting people and their property from unreasonable government intrusion;
- the Fifth Amendment, guaranteeing due process of law and exemption from self-incrimination;
- the Ninth and Fourteenth Amendments, which reinforce other rights and provisions in the Constitution.

In applying these long-standing guarantees in the burgeoning electronic forum, Tribe recommends that policymakers look not at what technology makes possible, but at the core values the Constitution enshrines. The overarching principles of that document, he maintains, are its protection of people rather than places, and its regulation of the actions of the government, not of private individuals. Other central values Tribe notes are the ban on governmental control

[2] *Proceedings of The First Conference on Computers, Freedom & Privacy.* Los Alamitos, CA: IEEE Computer Society Press, 1991.

of the content of speech; the principle that a person's body and property belong to that person and not the public; and the invariability of constitutional principles despite accidents of technology.

To insure that these values prevail as technology changes, Tribe proposes adding a 27th amendment to the Constitution to read:

> "This Constitution's protections for the freedoms of speech, press, petition and assembly, and its protections against unreasonable searches and seizures and the deprivation of life, liberty or property without due process of law, shall be construed as fully applicable without regard to the technological method or medium through which information content is generated, stored, altered, transmitted or controlled."[3]

Who Regulates and How

Speakers at the conference did not argue with Tribe's goal of an enlightened electronic communication policy on the part of the government, but some disagreed over who should be responsible for formulating that policy and whatever regulations accompany it.

Jerry Berman, a longtime privacy advocate who is now Director of the Washington office of the Electronic Frontier Foundation, warned that, in light of the courts' current record on civil liberties, any strategy giving them primary power to settle electronic speech disputes was dangerous. He argued instead for legislative controls.

Others worried that lawmakers, misunderstanding or misinterpreting existing electronic speech problems, would push through harsh and intrusive regulations. Steve McLellan, a special assistant to the Washington Utilities Commission, cited efforts in his state by phone companies wanting to institute caller ID systems. The companies lobbied for authorization of that technology by portraying it as customer protection, a way to combat obscene and crank phone calls. The constitutional privacy issues got buried in politics until the utilities commission announced that it would approve caller-ID tariffs only if they provided for blocking mechanisms provided free and at the discretion of the customer.

Yet another potential regulatory force was posited by Eli Noam, Director of the Center for Telecommunications and Information Studies at Columbia University. Noam suggested that computer-based information networks will become quasi-political entities, not subordinated to other jurisdictions, as they tax, set standards of behavior and mediate conflicts among their members, and band together to influence economic and social policy.

---

[3] *Ibid*, p. 12.

Current Regulation

There are myriad laws on the federal and state levels with potential impact in the electronic forum: the Privacy Protection Act, Freedom of Information Act, Wiretap Act, Paperwork Reduction Act, sunshine laws, obscenity laws, and laws regulating copyright, trademark, interstate commerce, and product liability. As New York attorney Lance Rose points out, this proliferation of laws tends to reinforce the most restrictive standard -- because computer users and service providers cannot inform themselves about all potentially relevant rules, they are well-advised to stay within the boundaries of the strictest regulation that may apply.

Congress has also passed legislation aimed directly at electronic communication within the government, including:

- the Computer Matching and Privacy Protection Act of 1988, which prohibits government agencies from combining discrete computerized personal records as a basis for taking adverse action against an individual until the results of the match have been verified independently;

- the Computer Security Act of 1987, designed to improve the security and privacy of federal computer systems;

- the Electronic Communication Protection Act of 1986, which safeguards electronic communication from interception, disclosure and random monitoring without a court order; and stipulates that a court order must be time-limited and must specify the information sought;

- the Computer Fraud and Abuse Act of 1984 (revised in 1986), which criminalizes unauthorized entry, and taking or alteration of information from computers; authorizes fines and imprisonment up to 20 years under certain circumstances; and gives the Secret Service authority to investigate potential offenses. In an effort to balance the punitive aspects of the Act, Sen. Patrick Leahy (D-VT) introduced an amendment to the 1991 crime bill that defines criminal liability in electronic communication cases as intent to damage, rather than as the technical concept of unauthorized access. The bill (S. 1322) will come up for a vote again in 1992.

Both the Computer Fraud and Electronic Communication Protection Acts include exceptions to their non-disclosure provisions for service providers who "may divulge" the content of a communication to a law enforcement agency if the contents "appear to pertain to the commission of a crime." Bulletin board operators have voiced concern over the ambiguity of this provision, questioning if it implies a duty on their part to report on the content of their boards.

THE ELECTRONIC FRONTIER: SOME SKIRMISHES

It is by no means a foregone conclusion among potential regulators of electronic speech that it is wholly protected by the First Amendment, but even if

that were agreed upon, the issue of how to determine the limits of what is permissible, desirable and necessary would still loom large. The discussion has been framed by a set of paradigms, in which the electronic forum is portrayed as a mix of the past -- the American frontier -- and a wholly new phenomenon, Cyberspace.

The term Cyberspace comes from William Gibson's novel, *Neuromancer*. It is the "place" telephone conversations and most financial transactions exist, the home of cyberpunks, and the bane of those who prefer to keep personal information private. Though subject to legal and social pressures, there is still something untamed about it, and so, a writer in Wyoming named John Perry Barlow coined the term "the electronic frontier."

Hoping to seize the initiative in taming this territory, Barlow teamed up with computer entrepreneur Mitch Kapor to create the Electronic Frontier Foundation (EFF). Since it began in July 1990, the EFF has provided guidance to legislators and courts about civil liberties on the frontier, and legal assistance to those whose liberties have been threatened.

Frontier Law

Even with much of its territory up for grabs, Cyberspace has been populated for some time, albeit by groups with widely divergent perceptions of the communal good. On one side are "hackers," a sometimes pejorative term, but used neutrally here to describe people who gain unauthorized access to computers for whatever purpose. These hackers see themselves as unfettered, adventuresome cowboys who, in keeping with the frontier myth, are being fenced in by the settlers -- the business interests who have staked claim to the terrain -- and by the law that tends to protect these established interests.

The cowboys defend computer hacking as a harmless pastime, as a pioneering activity that expands the boundaries of what is electronically possible, or as a political response to proprietary interests and individual profit. The settlers attack it as criminal, antisocial and malicious activity that costs everyone in money and security. By some estimates, computer crime accounts for as much as $5 billion in losses to government and business yearly.[4]

One of the most publicized cases of computer crime involved a virus (a software program that can alter data or erase a computer's memory) that was unleashed in 1988 over InterNet, an international computer network. The virus, known as the Worm, was written by Robert Morris, a graduate student at Cornell University, who claimed that he had created it as a prank before it got loose and infected thousands of government and academic computers. As a first-time offender, Morris was given a light sentence, but the principle established by the case has been allowed to remain: to get a conviction for computer abuse, the government need only prove unauthorized access, not intent to harm. This ruling

[4]Peter H. Lewis, "Can Invaders Be Stopped but Civil Liberties Upheld?" *The New York Times*, 9/9/90.

has been compared to punishing a trespasser for the more serious offense of burglary or arson.

The Morris virus not withstanding, the bulk of computer crime is not committed by hackers, but involves credit card fraud or theft by people within large companies, which are often reluctant to report it and publicize their vulnerability. In setting up the Electronic Frontier Foundation, Barlow and Kapor were reacting most directly to Operation Sun Devil, a part of a federal effort to combat computer crime, which had as its most visible targets young computer hackers and their systems of communication.

On May 8, 1990, armed with 28 search warrants in 14 cities, Secret Service agents seized at least 40 computers and over 50,000 disks of data from individuals they suspected of possessing illegally-obtained information. Only seven arrests resulted, although the government kept and searched the computers and software of more who were not charged. Information obtained by CPSR under a Freedom of Information request reveals that the Secret Service had been monitoring on-line communication and keeping files on individuals who had committed no crime for several years prior to the raids.

Steve Jackson Games

The February before the Sun Devil raids, a grand jury indicted Craig Neidorf, a student and the publisher of an electronic magazine called *Phrack*, for reprinting a document stolen from a Bell South computer. Three hackers had already been sentenced to prison for stealing the document, which concerned a 911 emergency system. The phone company claimed the document was highly sensitive and set its value at $79,499. When Neidorf's case came to trial that July, however, it was revealed that the document was publicly available at a cost of $30. The government dropped the charges, but the magazine had already ceased publication, and Neidorf had incurred about $100,000 in legal costs.

The Bell South file had been made available to bulletin board systems (BBSs) around the country, including one operated by an employee of Steve Jackson Games (SJG), a creator and publisher of computer games in Austin, Texas. While looking for evidence against the employee, Secret Service agents searched the bulletin board run by Jackson and found the draft of a rule book for a fantasy game called *GURPS Cyberpunk*. They decided it was a manual for breaking into computers.

On March 1, 1990, agents raided SJG and seized computers, drafts of the game, and all the information and private communication stored on the computer used for the bulletin board. Jackson was never charged with a crime, but none of his equipment or files was returned until nearly four months later. He was forced to lay off half of his employees and estimates that the raid cost him $125,000 in publishing delays. This is a small-scale equivalent of seizing the printing presses and files of *The New York Times* because the Pentagon papers were found on their premises; such raids are expressly forbidden by the Privacy Protection Act.

With the help of the Electronic Frontier Foundation, Jackson is suing the

Secret Service for violating his Constitutional rights. Specifically, his lawyers are arguing that the request for the search warrant caused a prior restraint of a publication, was misleading because it did not tell the judge that SJG was a publisher, did not meet the specificity requirement of the Fourth Amendment, and failed to establish probable cause that criminal activity was taking place. The case is in litigation.

Meanwhile, the EFF has been working on model search and seizure guidelines, which they hope to persuade the American Bar Association to adopt in place of its current guidelines for the issuance of search warrants relating to business records. In an attempt to make searches less intrusive and destructive, EFF recommends that:

1. computers used for publishing or electronic bulletin boards be afforded the same First Amendment protections as other means of publication;

2. in determining if just cause for seizure of equipment and software exists, judges shift the emphasis from what is technologically possible (e.g. an electronic trip wire that can erase all data) to what is likely to happen;

3. the search of computer disks take place on a business's premises, whenever possible;

4. under most circumstances, computers be seized only when they are the instruments of a crime.

Bulletin Boards

Electronic bulletin board systems are an increasingly pervasive mode of electronic communication and probably the most vulnerable to censorship. Part of the problem stems from a lack of definition. Are bulletin boards publishers, common carriers, broadcasters, electronic file cabinets, owners of intellectual property, private forums, libraries, newsstands, a combination, or none of the above? How they are categorized will determine if and how they are regulated.

BBSs are relatively new, dating from about 1978; today, as many as 60,000 may be operating in the U.S. Though most are small and specialized, the government operates several big ones, such as InterNet, and businesses run others, including the two largest: Prodigy (owned by IBM and Sears) and CompuServe (a subsidiary of H & R Block). These BBSs allow individuals to "log on" to a host computer by use of a modem and telephone lines. Once they are hooked up, users can participate in electronic conferences, or conversations, send electronic or E-mail to specific individuals, and "post" messages directed at a general audience.

Most BBSs neither monitor nor control E-mail, but many edit or otherwise restrict the messages on their bulletin boards. Some, such as the Whole Earth 'Lectronic Link (the WELL) in Sausalito, CA, place all responsibility for words posted on their system with the author, removing only clearly illegal or libellous material. The WELL community of about 5,000 members so far has regulated itself

effectively. Other systems are less tolerant.

In 1988, Stanford University attempted to block a jokes section of the bulletin board Usenet after becoming aware of an ethnically derogatory joke posted on it. The ban, though official policy, could not be implemented technically, and the jokes continued to be available throughout the campus. After a protest by students and faculty, the ban was lifted.

Prodigy has been more successful in controlling the content of its bulletin board. It claims the right to do so as a private company contracting with customers to deliver a service, and as a publisher selecting the content of its on-line publication much as an editor edits a letters-to-the-editor page. Messages are first scanned by a computer to catch words and phrases Prodigy deems offensive, then vetted by employees before being posted.

This editing has made for considerable controversy in Prodigy's three years of existence. In 1989, Prodigy cut out a section of its bulletin board called "health spa" after a yeasty exchange between homosexuals and fundamentalists. The next year, it banned messages from members protesting its pricing and editorial policies. Then this past year, the Anti-Defamation League publicly condemned the bulletin board for carrying grossly anti-Semitic messages. Prodigy responded that the messages were protected speech, but added the puzzling explanation that it made a distinction between derogatory messages aimed at individuals and those aimed at groups.

The question of what legal precedent to apply to bulletin boards moved closer to resolution with a court ruling late in 1991. In *Cubby v. CompuServe*,[5] an electronic newsletter called Skuttlebut claimed that it had been defamed by a competitor known as Rumorville, which CompuServe publishes on its Journalism Forum. A federal judge in New York likened electronic bulletin boards neither to publishers nor common carriers, but to distributors of information such as newsstands, bookstores and libraries to which a lower standard of liability applies. He decided, therefore, that CompuServe could not be held liable for statements published through its electronic library, particularly because it had no reason to know what was contained there.

ELECTRONIC INFORMATION AND PRIVACY

Private facts about individuals are much easier to gather and store on computer than on paper and are much more accessible to unauthorized scrutiny. Thus, computer monitoring challenges traditional expectations of privacy, exposes nearly every facet of an individual's life to potential public view and commercial use, alters the relationship between employers and employees, and opens the way for unprecedented government surveillance of citizens. For these reasons, concerns about the courts' vitiating the Fourth Amendment intensify

[5]No. 90 Civ 6571, 776 F. Supp. 135; Southern District of New York, 1991.

when computer-based communication and surveillance are involved.

Gary Marx, professor of sociology at MIT, notes ten characteristics of new kinds of computer-based monitoring that make them particularly intrusive:

> They transcend boundaries...that traditionally protect privacy. They permit the inexpensive and immediate sharing and merging and reproducing of information....They permit combining discrete types of information....They permit altering data. They involve remote access [which complicates accountability issues]....They may be done invisibly....They can be done without the subject's knowledge or consent. They are more intensive....They reveal previously inaccessible information. They are also more extensive and they cover broader areas.[6]

Privacy and Property

At a meeting of Computer Professionals for Social Responsibility held in Cambridge, MA October 1991, John Shattuck, Vice President for Government, Community and Public Affairs at Harvard University, noted that when the Bill of Rights was written, personal liberty was closely linked to private property. Thus, the Fourth Amendment protected concrete things and places from unreasonable government intrusion.

This idea was first upheld in relation to electronic technology in 1928, when the Supreme Court ruled in *Olmstead v. United States*[7] that the Fourth Amendment did not apply to wiretapping because telephone communication was not a material thing. (It was in his dissent on this ruling that Justice Brandeis defined privacy as "the right to be left alone.")

The principle of protection for tangible property remained largely unchallenged until 1967. Then, in *Katz v. United States*[8], the Supreme Court decided that the Fourth Amendment "protects people, not places," and was, therefore, applicable to wiretapping and electronic eavesdropping. This decision brought a person's ideas, politics and communication under the Amendment's protection for the first time, and set "reasonable expectation" as the standard by which to measure privacy rights. According to Shattuck, it also began a revolution in Fourth Amendment law.

From 1967 until the Electronic Communication Protection Act was passed in 1986, the only electronic communication covered by law was what could be

---

[6] *Conference*, p. 130.

[7] 277 U.S. 438 (1928).

[8] 389 U.S. 347 (1967).

heard. Nearly all computer-based communication remained outside traditional and legal privacy protections, even as it was becoming the dominant technology.

Much of digital communication in the U.S., including medical, insurance, personnel and retail transactions still lacks firm legal protection from intrusion, and the FBI recently proposed legislation that would require that all new telephone systems be designed to allow wiretapping, an ability the agency fears is endangered by new technology. In the privacy arena, the United States still lags far behind Canada, Australia and Western Europe, where at least six countries have a constitutional right to privacy and data protection.

Commercial Uses

The Fourth Amendment and the Privacy Protection Act apply only to the federal government, leaving commercial intrusion to be addressed piecemeal over the past two decades. For instance, the Supreme Court ruled in 1976 that there was no constitutional protection for personal information held by a bank because bank customers do not own these documents.[9] In response, Congress passed the Right to Financial Privacy Act two years later to create a statutory protection for bank records.

In 1977, the federal Privacy Protection Study Commission looked at the Privacy Act, seen then as a flawed compromise, and issued over 100 recommendations, many of which died at birth. However, one recommendation -- that the Privacy Act not be extended to the private sector, which should be allowed to comply voluntarily -- was more or less adopted by default.

Other laws have since been passed to control private access to personal information, including the Fair Credit Reporting Act (1970), the Debt Collection Act (1982), the Cable Communications Policy Act (1984) and the Video Privacy Protection Act (1988). Recently, Rep. Robert Wise (D- WV), chair of the Subcommittee on Government Operations, tried to establish a Data Protection Commission, but without giving it regulatory power.

As technology makes its easier to match databases and repackage personal information in commercially valuable forms, unease increases over the amount of information gathered and retained, where it comes from, how accurate it is, what use is made of it, and how individuals can control that use, especially when it is reused. Again, computers exacerbate the problem because they create a pervasive and long-lasting information trail that is decreasingly under the control of the individual involved.

Often there is no direct relationship between individuals and the keeper of information about them, as with credit bureaus. Other businesses, such as telephone companies and airlines, collect information routinely without external

[9] *United States v. Miller* 425 U.S. 435 (1976).

regulation of who sees the records or how long they are kept. Even when there is an intimate connection, as with medical information, the lack of legal protection allows genetic information and records of job-related injuries, for example, to end up in private databases that are available to employers and insurance companies.

Control over one's personal facts becomes even more tenuous when data collected by one organization are sold to another, which happens regularly without the individual's consent. This "second use" takes place primarily among businesses, but non-profit groups sell their mailing lists, and government agencies compare databases with businesses and each other: tax returns with welfare or student-loan records, for example. In 1991, Governor William Weld of Massachusetts proposed selling computer access to state Registry of Motor Vehicles records to private companies, but was dissuaded by vocal legislative opposition to the plan.

Privacy advocates are also troubled by deceptive data collection techniques and inaccurate information that can be difficult and expensive to correct. In July 1991, six state attorneys general sued TRW, one of the three big credit-reporting companies, for failure to correct major reporting errors. TRW eventually agreed to supply individuals with free copies of their credit files on request; other companies still charge for such reports.

Computers also provide a mechanism for fighting this Big Brother scenario. In 1990, Lotus Marketplace worked with Equifax, another consumer data collector, to put portions of its database onto compact disk so that marketing information about individuals could be sold in a convenient format to businesses. When the plan became public, it occasioned an outcry of surprising proportions -- about 30,000 responses, many from people who had learned about the project through electronic forums, and nearly all negative. In January 1991, Equifax and Lotus bowed to the pressure and scrapped the project.

Privacy Protections

For the past several years, privacy advocates have been working to pass policies and laws to protect individuals from the unwanted intrusions into their personal lives that computers make easy and appealing to businesses. The guiding principles for privacy policy are well summed up in a 1989 paper written by Jerry Berman and Janlori Goldman for the Benton Foundation:

> 1. Information collected for one purpose should not be used for a different purpose without the individual's consent.
>
> 2. Policy should be developed with an eye towards new advances in information technology and telecommunications.
>
> 3. Legal limits should be placed on the collection and use of sensitive information -- the more sensitive the information, the more rigorous the disclosure standard.
>
> 4. Individuals must be provided with easy access to their

records, including access to computerized records, for the purpose of copying, correcting, or completing information in the records.

5. Exemptions for non-disclosure should be clearly justified and narrowly tailored to suit the requestor's need.

6. Legislation should include enforcement mechanisms, such as injunctive relief, damages, criminal penalties, and reimbursement of attorney's fees and costs.[10]

Watching Employees

Also in the private sector, computers are increasingly being used to track employees' use of time, productivity, and communication with each other and the public. According to Karen Nussbaum, Executive Director of 9to5, the national organization of office workers, the work of 26 million employees is monitored electronically, and the evaluation and pay of 10 million is determined by computer-generated statistics. This kind of monitoring is more intrusive than human supervision, she points out, because it watches the personal habits of employees and because it is constant.[11]

As a form of surveillance, employers often reserve the right to read the electronic mail of employees and may do so because the Electronic Communications Privacy Act protects electronic mail only on public networks. The E-mail systems of large corporations, including Federal Express and American Airlines, automatically inform workers that the company may read mail sent over the systems. Other companies do not inform, but read anyway. When an employee of Epson America, a California-based computer company, learned that this was the company's practice and complained, she was fired the next day. Her lawsuit charging wrongful termination is in litigation.[12]

In the fall of 1991, Sen. Paul Simon (D-IL) introduced legislation (S. 516) which would require that employees and customers be notified if their electronic communication and telephone conversations are being monitored, either in specific instances or as a policy of their employer. Rep. Pat Williams (D-MT) has introduced similar legislation in the House (HR. 1218), and both bills are in committee.

Government Surveillance

---

[10]Berman, Jerry and Janlori Goldman, *A Federal Right of Information Privacy: The Need for Reform*; Washington, DC: Benton Foundation, 1989; pp. 25-26.

[11] *Conference*, p. 128.

[12]Glenn Rifkin, "Do Employees Have a Right to Electronic Privacy?" *The New York Times*; 12/8/91.

The United States government is the largest collector of information about people in this country and perhaps the largest keeper of personal information in the world. This information consists mostly of separate records, such as tax and social security files, but in a 1986 study, Congress's Office of Technology Assessment determined that, because these files can be matched and combined, a *de facto* national database on Americans already exists.[13]

Other information is gathered by surveillance. The FBI's National Crime Information System (NCIC) is a high-speed, computerized system containing criminal justice information, including Secret Service investigations, missing person files, and criminal histories or "rap sheets." The system began in 1967 and now runs about one million transactions each day. Information is maintained on a computer in Washington, DC, which is connected to each state and to 60,000 offices including those of sheriffs, prosecutors, courts, prisons, and military investigators. For instance, a police officer using the NCIC system to find out if a driver he or she has stopped is wanted for a crime can call up fingerprints and photos on the database to make an on-the-spot identification.

The NCIC is proud of the efficiency of its system and claims that it has built in safeguards against inaccuracy and abuse. Civil libertarians, however, have doubts. In addition questioning whether arrests for current actions should be made on the basis of past behavior, they point out that data on arrests may be stored separately from data on convictions, and that computers make it harder to control the spread of inaccurate, outdated or ambiguous information. They also fear that the ease in using the system will encourage police to be less discerning in stopping people for investigation.

There is concern too that the system can be used for purposes other than criminal justice, with information shared when someone applies for a government or military job or a professional license. In 1988, the FBI suggested connecting the NCIC to the computers of the Department of Health and Human Services, the IRS, the Social Security Administration and the Immigration and Naturalization Service; the plan was eventually defeated. More recently, alarms were raised by disclosures that the FBI conducted years of surveillance of political opponents of the Reagan administration's Central American policy, though they had committed no crime.

Library Awareness Program

On June 8, 1987, a clerk at Columbia University's Math/ Science Library was approached by two FBI agents who asked for information about "foreigners" using the library. This was, the agents said, part of the Library Awareness Program under which the FBI tried to enlist the assistance of librarians in monitoring the reading habits of "suspicious" individuals, variously defined as people with Eastern European or Russian-sounding names or accents, or coming from

---

[13] Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy*, 1986, cited in Berman and Goldman, p. 2.

countries hostile to the U.S.

It is still unclear how extensive the program is -- FBI officials have given contradictory information -- but the American Library Association (ALA) has verified 22 visits in various parts of the country that appear to have had the same purpose, and, in one statement, the FBI said the program was 25 years old. The FBI has also requested computerized check-out records from technical and science libraries and has asked private information providers, including Mead Data Central and Charles E. Simon Co., to help monitor use of their databases.[14] Although public and university libraries do not have classified information, the FBI has justified its interest in library use by a version of the "information mosaic" theory: that discrete and benign pieces of information can be put together to present a danger to national security and therefore need to be controlled.

Monitoring library usage is illegal in 44 states and the District of Columbia and violates an ALA policy, dating from 1970, that prohibits the disclosure of information about patrons' reading habits.

In July 1987, the ALA wrote the FBI to inquire about the Library Awareness Program, and the National Security Archive filed an FOIA request asking for records about the program. The FBI responded that it had no records under that name, and Quin Shea, who was then Special Counsel to the Archive, says they probably didn't, since the real name of the program is classified. The Archive filed a second FOIA request that September, and the ALA filed its own requests in October and December.

In September 1988, the ALA Intellectual Freedom Committee met with high-level representatives of the FBI. That same month, FBI Director William Sessions wrote Rep. Don Edwards (D-CA) that the program would be limited to technical libraries in the New York City area, presumably where the concentration of spies is greatest, and that cooperation of librarians would be voluntary. It was only in the summer of 1989, after Edwards and other members of Congress had gotten involved and the Archive had sued the FBI, that about 1200 pages of documents were released. These showed, among other things, that some librarians did cooperate. The Archive is again suing the FBI for the release of more material.

ACCESS TO GOVERNMENT INFORMATION

Privacy advocates and policymakers have long emphasized the importance of an individual's right to review information held about him or her. But, though the federal government has been collecting large amounts of information since the end of the last century, the public's right to monitor that information and the government's activities, has gained cache only fairly recently.

---

[14] *Newsletter on Intellectual Freedom* 9/88; p. 166.

The Freedom of Information Act (FOIA) was passed in 1966, and strengthened in 1974, followed in 1976 by the Sunshine Act. These laws gave the public greater access to information about government practices and decision making. Significantly, this swing toward openness in government took place at the same time that technological developments provided the government with ever greater information-collecting abilities.

Information policy, the means by which government information is made available, can be divided into three broad categories: disclosure, access and dissemination. The past decade has seen cutbacks in all three areas: for example, a 10% annual increase in classification decisions since 1982; the elimination or privatization of one in four government publications since 1981 under the Paperwork Reduction Act; and footdragging or outright hostility on Freedom of Information requests. In addition, the computerization of government operations has consistently been designed for bureaucratic efficiency with little interest in increased openness or access.

Electronic Access and Freedom of Information

One major area of debate in information policy is the effect of computerization on the FOIA. Theoretically at least, it is easier to search and retrieve records by computer than by hand, thereby lessening the burden on the responding agency and making them more amenable to FOI requests. But it is also likely that the volume and variety of requests will grow as the possibilities of information searches become apparent.

The Act mandates that records of the executive branch of government be available to the public on request, exempting only nine narrowly-defined categories, and it is almost universally accepted by now that electronic records are covered along with those on paper. There have been legal decisions to the contrary, which have placed privacy above disclosure concerns, but these have usually involved requests for information to be used commercially.

However, since the FOIA was written with paper records in mind, it left unaddressed the questions of what constitutes a record and a reasonable search, and what format is required for making information available. These and other disputes are currently being arbitrated by the courts, Congress and the agencies involved. The balancing act between access and privacy also becomes trickier with electronic storage of information. In 1977, the Supreme Court looked at a state's records of people who obtained prescription drugs legally and determined that this centralized file included sufficient safeguards to protect privacy, making it constitutional. Still, the Court found that government collection of personal information did pose a threat to privacy because "that central computer storage of the data thus collected...vastly increases the potential for abuse of that information."[15] A similar privacy concern informed a more recent Supreme Court decision in which the Reporters Committee for Freedom of the Press was denied

[15] ***Whalen v. Roe***, 429 U.S. 589 (1977).

access to FBI criminal history records in computerized form.[16]

In addition to arguing against disclosure on privacy grounds, the Justice Department has opposed requests for records analyzed and combined by computer, maintaining that this is equivalent to creating a new record, something the FOIA does not require an agency to do. Independent studies, however, tend to conclude that this is more like searching through an electronic filing cabinet and suggest that disputes be settled by applying a standard of reasonable effort, a term yet to be defined satisfactorily.[17]

A third major area of dispute is the form in which the requested information is made available. This problem arises in two different situations: where the data exist in more than one format and a requester has a preference, and where they do not exist in the format requested. The first is more common and more controversial. In 1984, a district court ruled that the government does not have to provide information in a requested format in order to fulfill its FOIA obligation (*Dismukes v. Department of Interior*, 603 F. Supp. 760 (DDC 1984)). But in *Department of Justice v. Tax Analysts* (492 U.S. 136 (1989)), the court determined that an agency can withhold a record only if it falls under one of the delineated exemptions. This ruling suggests that such a rationale would override *Dismukes* in a new court case.

In 1989, the Justice Department asked federal agencies how they viewed their obligations under FOIA to provide electronic information. The survey found wide variation among agencies, but a tendency against disclosure:

- 76% of the respondents did not think the law required them to create new, or modify existing, computer programs to search for requested information;
- 47% did not think they had to create new programs to separate disclosable from classified information;
- 59% did not think the FOIA required them to comply with the requested format.

Sen. Leahy is attempting to codify these requirements through a proposed Electronic Freedom of Information Improvement Act (S. 1939), which will come up for a hearing this spring. This amendment to the FOIA would require agencies to provide records in the form requested and make a reasonable effort to provide them in electronic form, if requested, even if they are not usually kept that way. It defines "record" to include "...computer programs, machine readable materials and computerized, digitized, and electronic information, regardless of the medium by which it is stored..." "Search" is defined to include automated

[16] *Reporters Committee for Freedom of the Press v. Department of Justice*, 489 U.S. 749 (1989).

[17] Harry Hammitt, "Formatting Freedom in the Computer Age," *Index on Censorship* 1/91, p. 30.

examination to locate records.

While many researchers and journalists support Leahy's bill, some public interest groups worry that, like other legislation targeting electronic communication, this will draw unwelcome scrutiny to the issue. Instead, they support an evolutionary process involving education and specific appeals to agencies.

Transactional Data and the IRS

The manipulation of data in a usable format is a useful tool in analyzing how government agencies really work. One particularly rich vein is transactional information, data recorded by government agencies in the course of their work. When this information is matched with other statistics, it can be analyzed to reveal what might otherwise be obscured about the activities of the government.

A successful practitioner of this kind of investigation is investigative journalist David Burnham. In ***A Law Unto Itself: Power, Politics and the IRS***, Burnham reports that computerized files obtained from the IRS revealed that audit rates vary widely among sections of the country, as does the likelihood of property seizure for delinquent taxes. He also discovered that there had been no increase in non-compliance rates over the past 15 years, although the IRS used the threat of increasing tax evasion as a basis for requesting new money for enforcement. The IRS had failed to adjust for inflation or margin of error in their calculations.

Burnham drew some of his conclusions from the work of Susan Long, Director of the Center for Tax Studies at Syracuse University. Burnham and Long founded the Transactional Records Access Clearinghouse (TRAC) with the goal of forcing the release of government data not available before. Long, who began her siege on the IRS in 1969, filed 13 FOIA requests to that agency and frequently took it to court to force it to open its records. She won a precedent-setting victory in ***Long v. IRS*** (596 F. 2nd 362 (9th Cir. 1979), with a ruling that the FOIA definition of "record" covered data on computer tapes. Her lawsuit, concerned the Taxpayer Compliance Measurement Program (TCMP), which measures the effectiveness of the IRS system and determines who will be audited. Although the data produced were kept so secret that they were withheld even from the Government Accounting Office, Long found that the information had little effect on the IRS's audit coverage, even when it pointed up regions or classes that were under-audited.

ENHANCING FREE EXPRESSION WITHIN THE ELECTRONIC FORUM

The dangers of assuming that because a technology is value-free and neutral, the uses to which it is put will also be benign are well-documented and real. But for all the new or magnified threats to individual liberties arising from computer-assisted communication, the electronic forum also offers the means to increase those liberties by expanding the possibilities for talking and working together and for building political and social alliances. Widespread and fairly allocated computerized resources can offer: increased citizen participation in

and oversight of government affairs; assembly, organizing and debate unrestricted by geographical distances or boundaries; decentralized decision making; a challenge to news and publishing monopolies; rapid international exchange of information; and individually-tailored, focussed information to combat the information glut that interferes with communication.

Stewart Brand has said that information wants to be free, and this may be nowhere more true than in electronic communication, which, by its very design, abhors censorship and monopolies (though history has proven that technology does not outsmart repression for long). It is important that those concerned with civil liberties enter the electronic forum with a mixture of optimism and vigilance and take part in the debate on its future while that debate is still open.

FOR FURTHER INFORMATION:

Berman, Jerry and Janlori Goldman. *A Federal Right of Information Privacy: The Need for Reform.* Washington, DC: Benton Foundation, 1989.

Berman, Jerry. "The Right to Know: Public Access to Electronic Public Information." *Software Law Journal* Summer 1989:491-530 (reprinted by The Markle Foundation).

Burnham, David. *A Law Unto Itself: Power, Politics and the IRS.* NY: Random House, 1989.

" " *The Rise of the Computer State.* NY: Random House, 1983.

Demac, Donna A. "The Electronic Book." *American Writer* Winter 1992.

Ermann, M. David et al. *Computers, Ethics, & Society.* NY: Oxford UP, 1990.

Index on Censorship July 1991. Section on computers and free speech.

"Is Computer Hacking a Crime? A Debate From the Electronic Underground." *Harper's* March 1990:45-57.

Lacayo, Richard. "Nowhere to Hide." *Time* 11/11/91: 34-40.

Office of Information and Privacy. *Department of Justice Report on "Electronic Record" Issues Under the Freedom of Information Act.* Washington, DC, 1990.

Perritt, Henry H. Jr. (prepared report). *Electronic Public Information and the Public's Right to Know.* Washington, DC: Benton Foundation, 1990.

Pool, Ithiel de Sola. *Technologies of Freedom.* Cambridge, MA: Harvard UP, 1983.

Proceedings of The First Conference on Computers, Freedom & Privacy. Los Alamitos, CA: IEEE Computer Society Press, 1991.

Reporters Committee for Freedom of the Press. *Access to Electronic Records.*

Washington, DC, 1990.

Rosenberg, Roni. Selected and Annotated Bibliography on Computers and Privacy. Palo Alto: Computer Professionals for Social Responsibility.

Scientific American. Special issue on communications, computers and networks. Sept. 1991.

Shattuck, John and Muriel Morisey Spence. *Government Information Controls: Implications for Scholarship, Science and Technology*. Association of American Universities occasional paper, 1988.

Westin, Alan. *Privacy and Freedom*. NY: Atheneum, 1967.

RESOURCES

ACLU Project on Privacy and Technology
122 Maryland Avenue, NE
Washington, DC 20002
(202) 675-2320
privacy issues

Computer Professionals for Social Responsibility
National Office
P.O. Box 717
Palo Alto, CA 94302
415/322-3778
general political and social issues

Electronic Frontier Foundation
155 Second Street
Cambridge, MA 02141
617/864-0665
general political and legal issues

National Writers Union
13 Astor Place, 7th floor
New York, NY 10003
(212) 254-0279
intellectual property issues

Public Citizen
2000 P Street, Suite 700
Washington, DC 20036
(202) 833-3000
privacy issues

Reporters Committee for Freedom of the Press
1735 Eye Street, NW, suite 504
Washington, DC 20006
(202) 466-6312
access to government information

Transactional Records Access Clearinghouse
478 Newhouse II
Syracuse, NY 13244
(315) 443-3563
access to government information

For more information, contact:
Gara LaMarche, (212) 972-8400 (o)
(718) 789-5808 (h)

* * *

This newsletter is a publication of the Fund for Free Expression, which was created in 1975 to monitor and combat censorship around the world and in the United States. It was researched and written by Nan Levinson, a freelance writer based in Boston and the U.S.

correspondent for Index on Censorship

The Chair of the Fund for Free Expression is Roland Algrant; Vice Chairs, Aryeh Neier and Robert Wedgeworth; Executive Director, Gara LaMarche; Associate, Lydia Lobenthal. The members are Alice Arlen, Robert L. Bernstein, Tom A. Bernstein, Hortense Calisher, Geoffrey Cowan, Dorothy Cullman, Patricia Derian, Adrian DeWind, Irene Diamond, E.L. Doctorow, Norman Dorsen, Alan Finberg, Francis FitzGerald, Jack Greenberg, Vartan Gregorian, S. Miller Harris, Alice H. Henkin, Pam Hill, Joseph Hofheimer, Lawrence Hughes, Ellen Hume, Anne M. Johnson, Mark Kaplan, Stephen Kass, William Koshland, Judith F. Krug, Jeri Laber, Anthony Lewis, William Loverd, Wendy Luers, John Macrae, III, Michael Massing, Nancy Meiselas, Arthur Miller, The Rt. Rev. Paul Moore, Jr., Toni Morrison, Peter Osnos, Bruce Rabb, Geoffrey Cobb Ryan, John G. Ryden, Steven R. Shapiro, Jerome Shestack, Nadine Strossen, Rose Styron, Hector Timerman, John Updike, Luisa Valenzuela, Nicholas A. Veliotes, Kurt Vonnegut, Jr., Gregory Wallance and Roger Wilkins.

The Fund for Free Expression is a division of Human Rights Watch, which also includes Africa Watch, Americas Watch, Asia Watch, Helsinki Watch, Middle East Watch, and special projects on Prisoners' Rights and Women's Rights. The Chair is Robert L. Bernstein and the Vice Chair is Adrian W. DeWind. Aryeh Neier is Executive Director; Kenneth Roth, Deputy Director; Holly J. Burkhalter, Washington Director; Susan Osnos, Press Director.