Chapter 11
Constitutional Rights

Contents

Chapter 11
Constitutional Rights

Introduction

Little legal precedent exists, in many cases, for applying constitutional law to the issues raised by computer-based information systems. As the courts begin to deal with the novel issues raised by the application of computer technology, they will probably attempt to apply traditional concepts. In this way, these new issues will become incorporated into existing legal precedent.

Legislative remedies may be called for when the courts do not find constitutional protections for threats to individual rights created by unforeseen technological developments such as television cameras, electronic wiretapping, and computer data banks. It is difficult to predict in advance precisely which computer-raised constitutional issues will create major legislative problems and which will be easily accommodated *in* the courts. Expert opinions vary widely, and little legal research has been done as yet.

The legal survey task of this study identified five areas of constitutional law that may be affected by information systems. These are:

- first amendment rights, which guarantee freedom of religion, speech, the press, peaceable assembly, and the right to petition for redress of grievances;
- fourth amendment rights, which guarantee against unreasonable search and seizure by the Federal Government;
- fifth amendment rights, which guarantee that a person may not be compelled to be a witness against himself or be deprived of life, liberty, or property without due process of law;
- sixth amendment rights, which guarantee the right of a speedy and public trial; and
- 14th amendment rights, which guarantee that a State cannot deprive any person of life, liberty, or property without due process of law nor deny any person within its jurisdiction the equal protection of the laws.

First Amendment

The principal purpose of guaranteeing freedom of speech is to ensure a free marketplace of ideas. Courts have tended to balance this freedom against other compelling social concerns, e.g., national security or public safety. For example, there have been a number of recent cases about the rights of reporters to protect their sources. However, certain characteristics of specific communication media affect how that goal is achieved.

The *printed page* is the least regulated communication medium. No Government interference in the content of published material is tolerated with the exception of some fairly limited and still contested restrictions in the areas of pornography, national security, libel, and trade practices. The relatively low cost and ubiquity of printing technology usually guarantees universal access to it for those who have something to say.

The *common carriers* are more restricted. Telephone and mail service are regulated monopolies that control the huge capital and institutional structures necessary to carry messages in various forms. Nevertheless, the communication capacity is very large. Without regulation, the potentiality would

exist that an operator might restrict a person's access to the medium. Regulation is therefore oriented toward assuring universal access by requiring carriers to provide uniform service to all at regulated prices. As with print, there are no limitations on message content aside from certain restrictions on pornography and other illegal activities.

The *broadcast* medium has a limited number of owners and operators as well as a limited capacity. Regulation must take into account the existence of these inherent restrictions on its use. Consequently, the thrust of the regulation is not the right of all to speak, but rather the right of all to be exposed to a "free market in ideas. " Under this interpretation, the Federal Communications Commission (FCC) has actively specified standards for broadcast content in such requirements as the "fairness" doctrine.

Cable services share both broadcast and common carrier characteristics, since their capacity is still limited but much greater than that of broadcast services. FCC, in its early licensing policy, required cable stations to provide public access channels that would be available to any potential user. (This requirement, among others, was rendered moot by a Supreme Court decision restricting FCC's authority to regulate in this area.)1 If cable providers have local monopolies over the delivery of information services to homes and businesses, there is a public interest in preventing the cable provider from exercising religious, political, or artistic censorship over the content.

Since the nature of first amendment protections is so strongly dependent on the characteristics of the media, it is reasonable to expect that new *information services* of the future will force the development of new types of policy. Some of the significant characteristics that may determine these policies are:

- *Restricted ownership and control of physical facilities.* Very high capital investments are required to install physical communication channels into homes and businesses. Even if competition in providing information services is encouraged, it is likely that there will be relatively few suppliers of facilities, * leaving the control over the physical communication lines to a few large organizations.
- *Much greater capacity.* The capacity of future communication lines into homes and businesses will be much greater than the current telephone and broadcast facilities. Cable and direct satellite broadcast lines will provide more channels and greater information capacity per channel. In addition, communication from the home back to the sender will be possible. Some limited implementations of two-way capability already exist, and expansion is likely over the next decade.
- *More producers.* The larger number of communication channels into the home coupled with low-cost national distribution systems are expected to lead to a proliferation of information producers and distributors beyond the current limited number of television networks.** Services such as those provided by the new "super stations" that operate nationwide over local cable networks, pay television networks such as Home Box Office, and upcoming direct satellite broadcast stations represent only the leading edge of such a trend in the entertainment area. In data communications, MicroNet and The Source are new services designed to link owners of personal computers with each

'*Federal ('communications Commission v. Midwest Video, 440* U.S. 689, 59 L.E. D. 2d 693, 99 Supreme Court 1435 (1979).

*The actual number of facility suppliers is growing (e.g., specialized common carriers and satellite carriers who supply a significant portion of their own facilities). However, this growth is much slower than that of the information producers.

**Th, new cable TV systems being built in the United States have up to 50 TV channels; some will have as many as 100 TV channels.

other and with larger computers, data banks, and information processing services over a nationwide network.

- *Low-cost access.* Network broadcasters pay thousands of dollars per minute to generate and transmit information. The new information and communication technology will substantially reduce the cost of distributing information. Therefore, it will be easier to enter the market, and a wider variety of information services will be made available.

The principal first amendment issue facing the Government will be to encourage the maximum freedom of expression—fostering the "marketplace of ideas"—in new electronic media that have been tightly regulated in more traditional forms. Factors that could work against this goal include pressures for Government censorship, monopoly in the production and distribution of certain kinds of programs and services, and excessive control over content by the operator or operators of the physical communication channels.

Another issue may serve to link first amendment rights with privacy concerns. Extensive data collection and possibly surveillance by Government and private organizations could, in fact, suppress or "chill" freedoms of speech, assembly, and even religion by the implicit threats contained in such collection or surveillance. [2] These threats might be directed as much at the "listener" as the "speaker. Clearly, automated information delivery systems possess a much greater capability of recording, storing, and analyzing in detail the flow of information from all sources into homes than do manual systems such as bookstores, newspapers, and the like.

As a consequence, consideration needs to be given to the distinction between information that is regarded by people to be private in nature and that which is public. Such a distinction may depend on whether the use of the information favors or is detrimental to the interests of an individual. For example, one does not usually attempt to keep secret the titles of books borrowed from a public library. However, an accurate profile of an individual's interests and attitudes could be provided by a complete dossier on that person's reading habits. Since computer technology has the potential capability of assembling such data bases, it may necessitate creating new definitions of the boundary between public and private information.

[2] Sam J. Ervin, "The First Amendment: A Living Thought in the Computer Age, *Columbia Human Rights Review*, vol. 4, No. 1, 1972, pp. 13-47.

Fourth Amendment

The fourth amendment protects the persons, houses, papers, and effects of individuals against unreasonable searches and seizures by the Federal Government. The study identified three significant areas in which new computer and communication systems may affect the interpretation and application of the fourth amendment.

1. the use of personal and statistical data contained in automated information systems as a justification for search and seizure;
2. the search and seizure of information per seas personal property, particularly in electronic form; and
3. the use of automated information systerns as a tool for search and seizure operations.

Justification for Data Collection

Criminal justice agencies have traditionally kept files that form the basis of their investigations. Depending on the system design, however, automation can change the nature of this recordkeeping in several ways:

- there are more individuals as data subjects;
- there are more data per individual;
- there is more centralization and correlation of diverse data sources;
- there is wider access to the data by more persons;
- there is faster access to the data; and
- there is more efficient remote access to the data.

Using the technology to the fullest capacity, it would be possible within the next decade for a policeman to obtain instantly a complete identification and dossier on an individual stopped in the street. As criminal justice information systems approach this capability, courts will become more interested in questions such as "reasonable cause" for such police actions as stopping and searching an individual. There is also the possibility of using statistical data as a basis for establishing probable cause.

In their concern, courts will probably look at issues of data quality. An erroneous record in a local manual file could cause an individual some distress, but an erroneous or incomplete record in a large, automated system with national or regional access could lead to more serious compromise of individual rights unless the record was promptly corrected. * This consideration combined with other related reasons could motivate courts to mandate that stringent data quality requirements must be met by automated systems before information from them could be used as reasonable cause for criminal justice actions.** In theory, checking and correcting records could be done more quickly with an automated system.

*In addition to the issues arising from the protections guaranteed by the fourth amendment, if access to the system were loosely controlled, and data used for purposes other than criminal justice such as employment or credit, serious harm could result.

* *The issue of data quality is explored in more detail in the OTA study on NCIC/CCH, in progress.

Information as an Object of Search and Seizure

The same information and information technology on which most institutions and people in this country increasingly depend for the conduct of their everyday lives are also becoming of greater importance to investigations conducted by the criminal justice system. Files, ledgers, correspondence, and address books have always been the objects of police searches in certain types of crimes. The criminal justice system will increasingly have to deal with their much more extensive computer equivalents, which may well raise new fourth amendment questions.

Two trends serve to increase the exposure of persons to searches. The first is that information previously unrecorded in any form will become collectable in computer data banks; electronic mail and electronic point of sale systems, for example, collect and store more data than the systems they replaced. The second trend is that data previously in the hands of individuals are now collected and stored by third parties, throwing the ownership of such data into question.

In a recent case,* the Supreme Court ruled that an individual's bank records belonged to the bank and were not protected constitutionally as his or her personal property. One basis for this ruling was that the use of a bank account was a voluntary action. Yet, it is questionable whether future participation in a computerized society can be construed to be voluntary if the alternative is to forgo all services necessary to live comfortably as a member of that society. Extensions of such reasoning could leave only a hollow shell of fourth amendment protection for personal records, while eroding any substantive effective barriers against Government intrusion.

As this happens, Congress will be asked to reestablish these protections legislatively. In the above cited case, a congressional act** addressed the problem of protecting

United States v. Miller, 425 U.S. 435 (1976).

**The Right to Financial Privacy Act (12 U.S. C. 340).

personal records held by financial institutions from access by the Federal Government.

The search and seizure of computerized records will probably present courts and legislatures with a number of problems in balancing the needs of law enforcement with fourth amendment protections. For example:

- When identifying records as objects of search and seizure, traditional standards that were reasonably effective with written documents may not apply when the information sought is buried in a very large, or even geographically distributed, computer data file.
- In its original or primary form, computer data is unreadable by human beings, Thus, seized evidence may be in a primary form, such as magnetic tape or disk, or it may be in a secondary form, such as printouts or charts. The status of this type of evidence may be contestable, particularly if a law enforcement agency is required to perform sophisticated file manipulation in order to pull out the particular information it is trying to introduce as evidence.
- If the information is in coded form (encrypted) and the key to its decoding (decryption) is only in the head of the suspect, fifth amendment protections may allow that person to withhold the encryption/decryption key or the encryption algorithm. Similar problems exist even short of encryption. Information can be hidden in a large data bank in such ways that it would be nearly impossible to find without knowing its precise location.

It is expected that the normal evolution of law in the courts will be able to deal with many of these problems as they occur. However, as the Miller case illustrates, the logical extension of legal principles into the information age can on occasion seriously alter the balance of power between individuals and and government, threatening protections included in the U.S. Constitution and Bill of Rights. In such cases, a legislative remedy will become necessary,

Information Technology as a Tool for Search and Seizure

Despite the difficulties of collating information that is dispersed and buried in very large geographically distributed computer files, national information systems may provide mechanisms for surveillance that penetrate more deeply into an individual's privacy than was previously possible.

In determining when fourth amendment protections apply, law enforcement distinguishes between "surveillance' and "search and seizure. There is no violation of this protection in observing an individual's daily public activity. It is the actual search of a person, a person's premises, or the seizure of personal records that requires warrants.

Information technology blurs the line between public and private activity. A nonelectronic mail cover requires approval by the Postal Inspection Service but not a search warrant because only the outside of an envelope is examined. In an electronic mail system, however, no distinction may exist between the "outside" (or address) and the "inside' (or contents) of a message. Therefore, it maybe difficult to distinguish a mail cover from a wiretap, which would require a warrant issued by a court upon probable cause, unless some form of coding could act to "seal" an electronic message as an envelope seals a physical one.

Similarly, the observation of shopping habits by following a person from store to store is surveillance. However, the use of an electronic funds transfer system to gather the same type of information would be far more intrusive, since much more data, some of it of a highly personal nature, could be collected in secret. The question is whether such transactions are to be considered public or private behavior.

The telephone created the possibility of wiretapping, which has stimulated numerous debates balancing the needs of law enforcement against those of individual privacy and fourth amendment protection. The courts and Congress have been struggling for some time with interpretations of the fourth amendment in terms of wiretapping. Information systems that provide such services as electronic mail and electronic funds transfer will likely provoke similar debates in Congress.

There is no doubt that access to computerized information could assist law enforcement in detecting crime and in prosecuting offenders. Consequently, the benefits afforded criminal justice will be a compelling argument. But no less compelling will be arguments citing the potential police-state dangers of widespread uncontrolled information surveillance of individuals.

This threat may become even more dangerous, since the surveillance of an automated information system can itself be automated, permitting an agency to keep tabs on large numbers of individuals efficiently. Ultimately, the information technology would permit both the tools and the opportunity for widespread surveillance of most of society. At present, the sizable amount of manpower needed to physically observe a person over a period of time acts as a check on such large-scale surveillance.

Finally, there may be a point beyond which a collection of comprehensive information about an individual, although comprised completely of information in the public domain, may assume the characteristics of private information. An individual's concept of private v. public information depends in part on the perception of its completeness and the ways it could be used against him/her.

Other Constitutional Issues

This study has identified several ways in which information systems are posing challenges to interpretations of the fifth, sixth, and by extension to States, the 14th amendments. (See beginning of this chapter for descriptions of these amendments.)

Managerial Due Process

More and more individuals are receiving an increased number of benefits and services from the Government. Information systems have become an indispensable tool for dealing with this growing workload (see ch. 8). To the extent that access to these services in a timely and fair way is a constitutional "due process" concern, the effect of information systems will be to increase scrutiny by the courts and by Congress of the "fairness" of the very large bureaucratic systems that will become established in order to operate service programs.[3]

The following questions about an administrative information system are likely to be of particular interest.

- Whether the information system provides for making timely decisions. While information technology can potentially speed bureaucratic processes, their implementation can often have the opposite effect.[4]
- Whether the information in the system is accurate and timely enough to ensure "fair" decisions. This question is similar to that of "reasonable cause' raised in the criminal justice discussion above.
- Whether there are subtle biases "built in" to the automated system that are invisible to the system operators and agency administrators because they are embedded in the code of the computer. Very large systems that "mass produce" decisions in such areas as health

[3] J. L. Mashaw, "The Management Side of Due Process," *Cornell Law Review*, June 1974, pp. 772-824.

[4] "DC Youth CETA Jobs Program Still Plagued by Delays in Pay," *Washington Post*, July 27, 1980, sec. 8, p. 1, col. 1.

benefits, student loans, or tax returns may react quickly to what the computer recognizes as "normal" applications, but reject "unusual" claims. If, as a consequence, clients are subjected to an unacceptable amount of hassle and delay, the definition of "normal" used by the computer may become subject to due process challenge.

Information Collection

The increased recordkeeping and data collection requirements imposed by the Government on organizations and individuals was one of the trends identified in this study. The quantity of information that individuals and organizations now must provide to the Government–either mandatorily (e.g., for census, tax, or regulatory purposes), in order to receive benefits (e.g., loan guarantees or medical payments), or to justify management decisions—is already extensive and growing larger.

There may be a threat to fifth amendment protections stemming from the use of personal or corporate computer data that have been collected by the Government for one purpose as evidentiary material in unrelated criminal or regulatory cases.

Social/Psychology-BaSed Applications

In addition to the straightforward uses of information systems to collect data and automate decisions, there are a number of new computer applications that use analytical techniques being developed in social psychology. The actual effectiveness of these techniques, which purport to predict and analyze human behavior based on the statistical analysis of information about individuals, is still being debated. Social scientists anticipate a steady improvement in the ability to predict future social behavior based on the analysis of seemingly unrelated personal characteristics or of the results from batteries of tests. If these capabilities improve as expected, some serious due process questions could be raised by their use in the criminal justice system. Three particular applications already appear to pose problems.

1. *Jury selection:* A small industry has grown up around the use of computerized dossiers of potential jurors along with computer models for predicting juror behavior. At this time, the technology is very expensive and its value is controversial. While some defense lawyers have claimed success owing in part to the use of these systems, it is hard to prove conclusively that the outcome of a particular trial was in any way due to specific juror selection.

   However, future computer technology will make this application cheap, and far more personal data about potential jurors will be available, legally or illegally. Furthermore, there is a sufficiently sound social scientific basis underlying this type of use to suggest that predictive techniques will be likely to improve in effectiveness. If so, the entire concept of an "impartial" jury as required by the sixth amendment may be challenged.[5]
2. *Lie detectors:* Lie detecting technology has already raised many difficult problems for Congress and the courts. Computer-based technology will add a new dimension to these still unresolved issues. So called "voice stress" analyzers are being manufactured and marketed for relatively low prices. This type of lie detector, which analyzes the degree of stress in a speaker's voice, depends on the assumption that measurable stress indicators appear when a lie is being told.

   Unlike older lie detector technology based on the polygraph, voice stress devices can be used without the cooperation or even knowledge of the sub-

[5] John I,. Wanamaker, "Computer and Scientific Jury Selection: A Calculated Risk, " *University of Detroit Journal of Urban Law*, vol. 55, winter 1978, pp. 345-370.

ject. This' single difference puts the use of lie detectors into an entirely new realm of fifth amendment problems, as well as opening up more generally new problems of social interaction in such areas as employer-employee relationships.

There are three distinct problems to be addressed: the effectiveness of such technology, the ways in which it is used by Government agencies and by police, and its use by employers, reporters and others for whom it would be both a tool for their work and a possible means of abusing individual rights to privacy.

3. *Predicting criminal behavior:* Much research has been done on the application of computer-based social science and statistical models to files of personal data and the results of psychological tests, in order to predict behavior. Techniques are being studied for detecting tendencies toward juvenile delinquency, drunken driving, or violent antisocial behavior, and for security checks by the Government. Conceivably, such research could be applicable not only to criminal justice problems, but also to such tasks as approving credit, determining insurability, or hiring and promoting employees.

As social scientists improve this predictive capability, important questions of fifth and 14th amendment rights will be raised. Essentially, individuals may be denied rights, privileges, and benefits based, not on past performance, but on a prediction of future tendencies. Courts will be examining these predictive models very carefully for their accuracy, relevance, and fairness. They will also be addressing the fundamental question of the appropriateness of these models and their potential for discrimination.

The problem will be to establish proper boundaries. Important decisions have often been based on estimates of an individual's future performance. An employee who does well in one job might be expected to perform equally well when promoted. On the other hand, society cannot imprison a person who a computer model predicts may someday rob a bank. But should that knowledge be "reasonable cause" to monitor such a person closely or deny employment?

New information system applications will increase the emphasis on drawing clear boundaries between what ways of using them are and are not acceptable. Particularly difficult equity issues will be raised if the results of such predictive models were to discriminate among groups that have experienced discrimination historically.