Chapter 7
Privacy

Contents

TABLE

Chapter 7
Privacy

Historical Context

Policy issues related to privacy date back many years before the existence of computers.[1] Such issues as the following have long concerned Congress and the Courts:

- Government intrusion–the right of the Government to physically intrude on the premises or in the belongings or personal effects of an individual.
- Surveillance of communication—the right of the Government to intercept communication by reading mail and monitoring telegraph traffic, by wiretapping telephone conversations, or by inspecting envelope exteriors to make a record of the senders (mail covers).
- Liability v. the first amendment–the right of authors to write—and publishers to print—within very broad limits, any information about a person or institution, whether such information is true or false, authorized or not.
- Privileged communication—the right of the Government to seek information conveyed under certain special circumstances, such as psychiatric treatment, religious confession, legal counseling, or media news-gathering.

These examples not only convey the historical nature of privacy debates but also the extraordinary range of issues encompassed by the term.

privacy as it relates to computers has been more narrowly construed. Historically, the principal discussion has been concerned with computerized banks of information about individuals, the collection of such data, and the uses made of it. A chronology of major events in the development of policy on recordkeeping practices is shown in table 6. In addition, a number of influential hearing records and reports have been issued by Congress.

Recordkeeping has not been the only area of privacy that has concerned Congress. Over the last two decades, hearings have also been held on subjects such as wiretapping, psychological testing of Government

Table 6.—Significant Milestones in the Development of the Recordkeeping Issue[a]

C. 1964	Proposal for a National Statistical Center and the resulting public debate on privacy and Government data systems—culminating in a series of congressional hearings.
1967	Alan Westin's influential book *Privacy and Freedom. b*
1970	Fair Credit Reporting Act—provisions regarding credit records on individuals. c
1971	Arthur R. Miller's book *The Assault on Privacy.' Computers, Data Banks, and Dossiers.* [d]
1972	National Academy of Sciences report: *Databanks in a Free Society.*[e]
1973	Health, Education, and Welfare Secretary's Advisory Committee on Automated Personal Data Systems report: *Records, Computers, and the Rights of Citizens.* f
1974	Family Educational Rights and Privacy Act controlling access to educational records. g
1974	Privacy Act of 1974 enacted. [h]
1977	Privacy Protection Study Commission report: *Personal Privacy in an Information Society.*[i]
1978	Right to Financial Privacy Act of 1978 enacted to provide controls on release of bank information.[j]

[a]Note: There were also numerous hearings and reports by Senate and House congressional committees during thls period which are not listed here. James Rule and collaborators list 60 major Committee hearings and reports dealing with information privacy from 1966 to 1977 [k]
[b]Alan West In, ***Privacy*** *and Freedom New* York Atheneum, 1967
[c]Fair Credit Reporting Act, 15 U S C 1681 (1970).
[d]Arthur R. Miller, *The Assauly on Privacy: Cornputers Data* Banks, and Dossiers (Ann Arbor University of Michigan Press, 1971)
[e]Alan Westln and Michael Baker *Databanks in* a *Free* Society (New York Quadrangle/New York Times Book Co 1972).
[f]Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records. Computers and the Rlghts of Citizens,* Washington D C 1973
[g]Publlc Law 93568
[h]Public Law 93579
[i]Prlvacy Protect Ion Study Commission, Personal *Privacy* in *an Inforrnation Society* Washington D C 1977
[j]Rlght to Financial Privacy Act of 1978 (Public Law 95-630)
[k]James Rule, et al., *The* Politics *of Privacy (New* York Elsevier North Holland. 19801

SOURCE: Office of Technology Assessment

[1]David J. Seipp, *The Right to Privacy in American History,* Harvard University Program on Information Resources Policy, P-78-3, 1978.

employees, and the use of polygraphs. Privacy issues have also been raised by congressional committees concerned with the data systems run by various agencies, in particular the Federal Bureau of Investigation (FBI), the Internal Revenue Service (IRS), the Social Security Administration (SSA), and the Census Bureau.

Privacy-related issues will remain on the congressional agenda over the coming decade for a number of reasons. [2]

- new computer and communication technologies will create new problems and change the nature of old ones;
- the public's awareness of and sensitivity to the privacy problems presented by large data systems appear to remain high; and
- the Federal Government has deliberately chosen to react to privacy issues associated with recordkeeping on a case-by-case rather than on an omnibus basis.

[2] L. Hoffman (cd.), *Computers and Privacy in the Next Decade (New* York: Academic Press, 1980).

Future Privacy Issues

An Omnibus v. A Selective Policy

Omnibus legislation, which would cover all data systems both public and private in which personal information is maintained, is the approach European nations have taken. In the United States this approach has been rejected by the Privacy Commission and the executive branch for several reasons. First, there would be serious difficulties in drafting such legislation in a way that would achieve the desired protection without seriously hampering legitimate data processing applications. Furthermore, the variety of systems, of applications, and of environments, ranging from large banks and insurance companies to street corner drugstores and individual homes, would be hard to accommodate with any single piece of legislation.

In addition, omnibus legislation could lead to the creation of another Federal regulatory agency that would exercise oversight over the information industry. Again, because of the wide variety of applications such an agency would find itself involved in most aspects of American life. The Swedish experience is often given as an illustration. In that much smaller country, a newly created data bank licensing board had 20,000 applications to process in its first year of operation.

With the selective approach, however, Congress will be considering a long series of privacy bills. A substantial legislative effort will be required to catch up with current computerized recordkeeping practices. An immediate concern is the development of privacy rules for computer applications in banking, medicine, social and medical research, credit, insurance, and criminal justice. Privacy is also likely to be a major issue in the development of electronic mail.

Furthermore, new applications for computers and communications, such as an automated securities exchange, in-home information services, electronic publishing, and the automated office, may create new environments for privacy policy issues to arise. As Government agencies such as the Department of Justice, IRS, or SSA begin to use the new generation of information technology for their recordkeeping activities, privacy problems that were not specifically addressed in previous legislation may have to be dealt with by Congress. Recently, for example, the availability of low-cost data communication technology has raised the message-switching issue to prominence in the congressional debate over the future of the operations of the FBI National Crime Information Center Computerized Criminal History system.

Unlike the executive branch, which can subject all proposed privacy legislation to a consistent agency review, Congress considers the different bills in a variety of committees depending on the applications and users under consideration. Therefore, careful coordination and the adoption of principles for guiding the nature of Federal policy concerned with the handling of personal information in automated information systems is needed in order to prevent the enactment of a patchwork of contradictory privacy legislation.

This approach leads to legislation tailored to the needs of the specific sector affected by it. However, there are also hazards. A danger inherent in disorganized privacy legislation is that businesses that operate in areas of overlapping authority would face a variety of regulations, some even contradictory, governing their data systems. Others might be able to find loopholes by operating in the gray areas between regulated sectors, thereby seriously abusing the intent of Congress.

Because the selective approach differs so radically from the approach taken by most other developed nations, problems could arise internationally. Many developed nations, for example those in the Organization for Economic Cooperation and Development, are attempting to coordinate their privacy legislation so that differences in their rules and practices will not hamper the exchange of information across their borders (see ch. 12). The rejection of an omnibus approach, coupled with the lack of a centralized authority over data banks, is making it difficult for the United States to enter into these international agreements. Such a divergence could leave the United States as "odd man out" with respect to transborder data flow. This could have serious implications for trade and international relations and warrants serious attention. [3]

[3]Donald Marchand, " Privacy, Confidentiality and Computers: National and International Implications of U.S. Information Policy, " *Telecommunications Policy*, September 1979, pp. 192-208.

Collection of Data

In an attempt to decrease the amount of data collected by Government agencies, Congress specified in the Privacy Act of 1974 that data collected must be "relevant" to the purposes of the collection. The Privacy Protection Study Commission reported finding a slight decrease in data collection following this legislation.

However, the relevancy test is undeniably weak and difficult to enforce, and the small decrease found in data collection was a one-time phenomenon. Recordkeeping is increasing, both in the Government and in the private sector. Furthermore, as more and more transactions in the private sector become automated, data that would normally not have been collected or retained will now be entered into computer systems and stored, thus becoming available to data collectors.

The recent dispute between Prudential Insurance and the Department of Labor (DOL) over access to personnel tapes is illustrative.[4] To investigate possible discrimination in hiring, DOL has requested complete personnel records held by Prudential. Without judging the merits of the case, it can still be observed that, were the files in question not integrated on magnetic tapes, DOL would have been unlikely to make such a sweeping request because of the burdensome task of analyzing manual records. It should also be noted that computer technology allows such files to be easily processed to create new tapes containing only the information DOL and Prudential would mutually agree is pertinent.

Relevancy is also a weak requirement with respect to its application to the timeliness of data. The Privacy Commission found that agencies were not particularly inclined to cull their files. As the cost of memory continues to drop and very large data systems become easier to operate, even existing economic and managerial incentives to clear

[4]"Prudential Barred From U.S. Contracts," *The Washington Post*, July 29, 1980, sec. A, p. 1.

data bases of old and useless information disappear.

A fundamental assumption underlying much of the privacy debate in the 1970's was that collecting personal information is in the nature of a transaction—the individual yields personal information in exchange for some benefit. Thus, much of the fair practice doctrine centers on the requirement that the recordkeeper abide by obligations implicit in that transaction. However, individuals will increasingly be encountering computerized systems that collect and store information about them without their knowledge or consent. Very few laws exist pertaining to the ownership or disposition of such information, even when its use may be contrary to the individual's perception of his or her best interests.

The mailing list systems were among the involuntary systems studied in depth by the Privacy Commission. Persons have no idea whether or how information about themselves is being compiled. Since, at the time of the study, the Commission deemed mail solicitation to be a socially benign activity, they did not consider this type of recordkeeping to be of serious concern.

However, pressures from users of such systems for greater selectivity in their mailing lists has led to collection of more personal data on individuals. Political solicitation lists, for example, may contain information about a person's organizational affiliations, religious beliefs, charitable contributions, income, and history of support for various causes. This type of information can be used to predict the likelihood that a person would support a particular candidate or political cause and is, therefore, useful in compiling a targeted mailing list.

Such personal information, which is often collected without the consent of the subject through the exchange or purchase of mailing lists or access to other open sources of information, assumes the character of a political dossier. It is not clear that existing controls, either over the use of such data systems for purposes beyond computing mailing lists or over the original collection of the information, are adequate to deal with the increasing capability modern technology offers to collect data and compile such lists.

Modern computer technology through the 1980's will facilitate the collection of personal data, as well as make possible its instantaneous nationwide distribution. Point-of-sale systems are an example of this trend. A sale made at a store and recorded through a terminal will collect a variety of information about a customer, such as what was purchased, the exact time and location of the transaction, and possibly the customer's financial status. This will not only be recorded at the bank, and thus fall under bank privacy rules, but may also be retained by the store management for its own use, or perhaps even sold to third parties.

Access

The controls in current privacy legislation that concern access to Government-held data by other agencies depend on a "use" rule. That is, with some exceptions, data may not be given to a third party for any purpose other than one "compatible" with that for which such data were originally collected, Such routine uses must be made known to the data subject either at the time the data is solicited from him or constructively through publication in the Federal Register.

The Privacy Protection Study Commission found this rule to be relatively ineffective. The word "compatible" is vague and subject to a variety of agency interpretations. In addition, there are a host of exceptions, both within the Privacy Act and in other laws, governing the ways in which agencies exchange information. The provision of notice was found to be equally ineffective. Finally, privacy rules conflict with freedom of information laws. For example, Iowa's attorney general recently ruled that the State's open records laws superseded

any rights to user privacy with respect to library records. '

The proliferation of personal data collection without either the subject's permission or knowledge implies that even if such a use provision were extended to the private sector and its ambiguities clarified, its effectiveness would be limited. The rule assumes a voluntary relationship between the primary data collector and the subject, and a willing yielding of personal information. Where such an agreement does not exist, the subject of the data is not the "owner" of the information.

The data collector argues, usually correctly, that the information being collected is already in the public domain. The issue may boil down to the difficult question of whether a compilation of information in the public domain along with statistical inferences drawn from it can become so comprehensive as to constitute an intolerable invasion of an individual's privacy. Some States are already considering bills to restrict the access to public records, in particular to auto licensing data.

OTA's study of the FBI's National Crime Information Center/Computerized Criminal History (NCIC/CCH) record system documents the difficulty in enforcing access rules for very large distributed information systems that serve many users and contain information of value to a variety of people. Even if tight security measures could solve the difficult problem of stopping access by unauthorized persons, no controls within the system can keep the data, once extracted by an authorized user, from being used improperly.

Furthermore, the overlap of authority (in the case of NCIC, between Federal, State, and local agencies), along with the concomitant overlapping assortment of rules and procedures, means that it is very difficult to establish a single consistent policy for accessing and using data.

'How a Libraries Fight Scrutiny of Borrower Records," *The Washington Post*, Dec. 2, 1979.

This problem is duplicated in the private sector. Retailers of personal data, such as credit bureaus or mailing list operators, have no control over how the information they sell is used. Large corporate information systems, where many employees or even outside users have access to the data, will have similar problems of control.

The question is not just the adequacy of the security of the internal system against unauthorized use, but who is authorized access to the data and how they use it. Many new information systems are characterized by their wide distribution and easy accessibility over communication lines. In fact, they are designed for just these characteristics. In such complex environments, with multiple data bases in the system and multiple users accessing it from anywhere in the Nation, procedural control of data use could be almost impossible.

A final access problem, suggested above, is the impact on privacy of the computerization of traditionally public Government files. Lists of property transfers, licenses, births, deaths, and so on have always been open, but difficult to get at and use. Certainly, they have not been easily absorbed into privately held data bases. Computerized files have changed that access capability, and as a market for such information develops the interest in using it will likely increase.

Microprocessors and Surveillance

The potential now exists for the development and marketing of a wide variety of devices either specifically designed or capable of being used for the surveillance of individuals without their consent. Microprocessor technology is progressing to the point where it will be common for computer logic and data storage capability to be built into inexpensive consumer goods of all kinds. Pocket-size, voice-stress "lie detectors" are already being marketed, although their reliability is unproven. Within a few years, wristwatch-size units will be available. Although at least one State, Penn-

sylvania, has a law requiring subject consent for use of such devices, its enforcement would be quite difficult when the possession and use of a unit can be so easily hidden.

Currently available security systems based on magnetic cards and microprocessor-based locks allow an employer or building manager to keep detailed records of the whereabouts of anyone in the building. Devices called "pen registers" provide a similar capability for monitoring telephone traffic. If voice recognition and picture processing capabilities improve as much as some experts expect over the next decade, other forms of inexpensive automated surveillance will also become available.

Abuse of this technology for illicit purposes may become a serious problem. However, seemingly legitimate applications such as retail market surveillance of customers or employer surveillance of employees may also cause concern if there are obvious abuses, Arguments for socially sanctioned uses will raise, in new forms, classic issues of civil rights v. both law enforcement and the rights of employers to monitor their employees. In this debate, the new information technology places powerful new tools in the hands of those who argue for greater social control.

The Glass House Society

The issues that are likely to remain active during the next decade or two arise from the public's misgivings that the use of large data systems containing personal information is threatening to them. Recent polls have shown a steadily rising concern over privacy, which is directed equally at Government and private data systems.[6]

Some social and political scientists suggest that the computer represents to the public the growing power of Government and other large organizations over their daily lives.[7] Thus, as the use of these information systems grows, the public's apprehension is also expected to grow as will pressures on public officials to control or even to stop certain types of computer applications.

There appears to be a trend toward a society in which information about a person's finances, medical and educational histories, habits as a consumer, daily movements, and communications with others through the telephone or the mail will be collected, stored in a computer, possibly sold to others, and used in ways over which the individual may have little or no control. There may be many benefits in terms of the productivity and efficiency of institutions, and in terms of broadened awareness and choices available to individuals as citizens and consumers. But the long-term social and political effects of this trend–beneficial and adverse—are still largely unknown. It seems likely, however, that they will be profound, and will alter how individuals both perceive and relate to the institutions that affect their lives. Consequently, Congress will continue to be a principal forum in which these conflicts will be deliberated and ultimately resolved.

---

[6] *The Dimensions of Privacy: A National Opinion Research Survey of Attitudes Toward Privacy* (Stevens Point, Wisconsin, 1979) for Sentry Insurance.

[7] James Rule, et al., *The Politics of Privacy* (New York: Elsevier-North Holland, 1980).