DATA BANKS, PRIVACY, AND SOCIETY

Willis H. Ware

November 1973

P-5131

The Rand Paper Series

Papers are issued by The Rand Corporation as a service to its professional staff. Their purpose is to facilitate the exchange of ideas among those who share the author's research interests; Papers are not reports prepared in fulfillment of Rand's contracts or grants. Views expressed in a Paper are the author's own, and are not necessarily shared by Rand or its research sponsors.

The Rand Corporation
Santa Monica, California 90406

Willis H. Ware

Data Banks, Privacy, and Society

Computer technology provides society with the tool it needs to accommodate growing information requirements. It lets us keep the records we have to keep, economically and efficiently. But the computer-based automated file can also work against us. The information in computer systems can be valuable and thus subverted for inappropriate purposes. Because of this vulnerability, automated data systems add a new dimension to the problem of personal privacy, as well as provide opportunity

*This paper was originally published as an essay in the Rand 25th Anniversary Volume, The Rand Corporation, November 1973.

for embezzlement, blackmail, and other fraudulent schemes. Our essential tool could become a major societal threat unless we provide effective safeguards to protect personal information in automated files and those to whom it pertains.

The attitude of the public with regard to personal information has changed in recent years. We are becoming increasingly aware of data files and the information they contain about us.

To some data systems we provide personal information voluntarily. We do this in exchange for some benefit, privilege, or opportunity: we want to make credit-card purchases, obtain loans, write checks, get a passport, apply for a job. Some information we provide because it is required by law: we participate in the census or fill out questionnaires for military service. Sometimes we provide information inadvertently: we are in an accident that involves a police record.

We provide considerable information because we ask for services from government. We want educational assistance, unemployment support, housing allowance, or care for the older segment of the population. Congress, in turn, insists on strict accountability of public assistance programs and on evaluation of the success of such undertakings; this requires personal records and computer processing. The more extensively we and the government interact, the more extensive must be the records that need to be compiled and maintained by computer.

INFORMATION NEEDS OF GOVERNMENT

As our population increases and our society becomes more complex, and as the government enlarges its range of services, the need for personal information grows. The federal government, for example, needs extensive information in order to formulate new legislation, to adopt sound fiscal and tax policies, for entitlement decisions with regard to public assistance programs, to estimate the consequences of a possible decision, and to generally conduct the affairs of the country.

In the face of increased demand for natural resources—and many man-made resources—comprehensive planning becomes crucial at all levels of government. To adequately balance

quantity and demand for land, energy, water, highways, etc., government regulation and intervention are required. Local governments need information to regulate land use, and to plan sewage and water facilities, transportation, and many other public services.

Industry gathers much personal information in order to assemble and maintain the records that are required in an era of intricate labor relations, widespread union practices, pension and insurance plans, state and federal tax withholding, and other regulatory and legal restrictions. Social research is also increasing, and along with it social experimentation, so that more information about people, their behavior, and their habits must be gathered. Thus, there exist numerous automated files containing extensive personal information about all of us.

ACCESSIBILITY OF PERSONAL INFORMATION

For whatever reason we furnish information about ourselves, we implicitly tend to assume that it will be used only in our best interest and solely for the purpose for which it is furnished. Thus it comes as a surprise when we find that the information we have provided for one purpose is being used for a different one. As a result of personal data submitted for a driving license, for example, we find ourselves on a mailing list and inundated with advertising literature.

While much personal information in automated files is anonymous, describing in a statistical way some characteristic segment of the population, there is also much that is identifiable in order to permit decisions to be made based on a person's record. Given our mobility in residence and employment, many organizations find it expedient to exchange data or to transport information about an individual from one place to another. Thus the automated record system tends to concentrate information about people in one place and to provide ready accessibility to it for a wide group of users. Moreover, automated systems can, in principle, exchange data automatically with one another and so broaden the exposure of personal information. Such linking of files, when it occurs, enlarges the volume of data available to any one inquirer.

Of the many files containing personal, private information, a considerable number are at government level: census data, social security records, Internal Revenue Service tax records, various research collections in the social and life sciences, etc. Some are in the financial industry: bank account records, savings and loan records, stock investment records, credit records. Many relate to health care, such as hospital, medical, or psychiatric records. A few have been collected by the recreational and leisure-time industry in the course of making reservations and travel plans. Those accumulated by educational institutions include a complete, detailed account of performance in high school and college.

SOCIAL SECURITY NUMBERS AS IDENTIFIERS

If the file is for a local purpose, it may be sufficient to identify the individual by his name and address. Often some secondary identification is included; the mother's maiden name is one traditional example. In many instances, federal statutes require that a person's social security number be given as an authenticator of his identity; financial institutions, for instance, are legally required to obtain it.

Federal statutes or regulations will, in some cases, authorize the exchange of information among data banks. The Internal Revenue Service, for example, regularly exchanges data with state tax-collection agencies; and in so doing, ensures that identity is preserved and records are kept straight by means of the social security number. In other cases, an administrative action will stipulate that social security numbers must be obtained. They are required by the Department of Motor Vehicles in some states, for example. Occasionally, social security numbers are secured for no particular purpose other than as a hedge against an unknown future need. Some educational organizations use them as student identifiers.

Unfortunately, the growing number of automated files in which a record about an individual includes his social security number implicitly encourages the exchange of information; it also serves as a key for combining information from several sources. Sometimes, exchange of data is facilitated by freedom-of-information acts at both federal and state levels,

because these acts require that public information be provided to any requester. A person who finds himself in a file considered to be public information has no effective control over how his information will be used.

While linkage among information systems is undoubtedly not yet so widespread as to be considered at the critical level, many factors suggest that the situation is likely to develop: the remote-access computer systems that service geographically distributed users; the awareness by a manager or an official that information from some other sources will help him do his job better; recognition by a researcher that combinations of files will give him more insight into his problems; and the economic efficiency of combining several small information systems into a large one serving many classes of users.

CONTROL OF PERSONAL RECORDS

With this growing awareness that automated files pose a real threat to personal privacy, we are becoming more sensitive to the misuse of personal information, and are willing to complain about it. Our complaint may simply be the result of a personal annoyance—a dunning letter received because a paid bill has not been accurately posted to the correct account; but the complaint can be much more serious. Because of incomplete or erroneous information in an automated file, we may suffer a damaged reputation, loss of financial status or position in the community, the denial of credit, the loss of a job, or improper arrest.

Public concern over the invasion of personal privacy may well rest more on a sense of having lost control—of not knowing when information freely given for one purpose will be used for another—than on the feeling of being surrounded by a data-hungry environment. We feel a need to be guaranteed that personal, identifiable records will be used in ways over which we have some control—and that we have a mechanism to seek recourse in case we should sustain harm if they are improperly used.

The Constitution of the United States does not *specifically* provide for a right of personal privacy. Justice Brandeis,

dissenting in the case of *Olmstead* v. *the United States* (1928), first suggested that personal privacy is implied in the Constitution. A continuing series of judicial interpretations have cumulatively created the right of privacy. The legal basis for these judgments includes the first amendment guarantee of free speech, press, assembly, and religion; the third amendment prohibition against quartering soldiers in private homes; the fourth amendment right to security from unreasonable search and seizure; the fifth amendment right against compulsory self-incrimination; and the ninth amendment guarantee of other unenumerated rights retained by the people.

Recent Supreme Court decisions have declared the right of personal privacy as the basis for protecting such freedoms of an individual as the practice of contraception or the reading of pornography in the home. Unlike the United States, other countries—Canada, for example—have not developed a constitutional or legal basis for extending personal privacy to its citizens.

From the standpoint of the individual citizen, he is generally unaware that information about himself is being disseminated without his approval; in most instances he is powerless to stop it even if he should discover it. Since large information systems are a relatively recent development in a technical and operational sense, one can expect to find inadequacies in their designs or incomplete operational practices, either of which can be manipulated to steal information, or can result in inadvertent or malicious leakage of information to someone not authorized to have it. Furthermore, information in data banks is usually not protected against legal process. While specific legislation does sometimes protect information in automated files, or authorizes a government official to extend protection as he sees fit, by and large, the bulk of information in such files is subject to confiscation through administrative or legal subpoena or through other court-directed seizure.

HOW TO ACHIEVE PROPER BALANCE?

Thus the exploitation of computer and communication technology in modern recordkeeping systems highlights the

central confrontation between the need of government and business organizations to have personal information for efficient planning and operation and the need of the individual to have control over the way in which information about himself is used. How can we achieve a more satisfactory balance?

There are actually two quite different issues involved. One is the technical problem of designing and implementing an automated information system that will safeguard the data it contains. A properly designed system will not inadvertently leak information, and it will be physically protected against pilfering, thievery, and infiltration. It will deliver information only to users authorized to have it.

The other issue is the much more difficult one of controlling what personal information should be collected in the first place, of determining who shall have access to it and for what purpose, and of giving the individual more control over information about himself. Unlike the control exercised over national security information, there is no classification scheme established by law or executive order for labeling personal information as "sensitive," "nonsensitive," or "ultrasensitive"; nor are there any government-wide guidelines for establishing who may have access to it. Thus, the rules and regulations governing dissemination of personal information from a file tend to be made by the individual or organization that collects the data and owns the file. In many instances, there are no established practices to serve as a model for good procedure. In the particular case of consumer credit reference systems, the Fair Credit Reporting Act does impose limited constraints; for example, provision is made for the individual to inspect his file and to correct it.

SOME SUGGESTIONS FOR SOLVING THE PROBLEM

In solving the technical problem, physical protection, computer hardware and software safeguards, communication security safeguards, and a general management-procedural overlay are collectively necessary to provide the overall protection needed. In all of these areas, the requirement of the defense community to protect classified information is a

driving force for research, new system designs, and general progress toward an eventual solution. Fortunately, many of these same safeguards are needed in any computer system that shares its resources among many users—that is, the time-shared computer system—and to this end the general advance of the computer industry will help to provide the technical basis needed.

In solving the problem of restricting the collection of personal information, of controlling its dissemination, of carefully specifying what use may be made of it, and of affording the individual greater participation in the dissemination of his personal information, various suggestions have been made but none have been generally implemented. To improve the care with which recordkeeping systems are designed and operated, one proposal is to certify computer programmers and system designers. This action would assuredly be a useful one; but unlike the older engineering fields, the computer field does not yet have a well-established body of preferred practice upon which to draw. Thus, while certification would be a helpful step, it would put the responsibility for a properly designed and controlled record system in the wrong place. The responsibility should be assumed by the organization that assembles the system, initiates its design, and operates it, not by the technician who implements it. While certification is a step in the right direction, it cannot of itself adequately solve the problem.

A second solution might be the ombudsman approach, which has been used for many years in Scandinavian countries. Basically, the ombudsman is a spokesman for an individual who has been harmed; he serves essentially as a communication channel between the person and the bureaucracy in matters of dispute. While the ombudsman concept is a useful third-party mechanism to facilitate resolution of argument, it is not a well-established mechanism in the United States nor can it function as a sufficiently strong force to be a solution for the entire problem of protecting personal privacy.

A third solution, one that attempts to deal with the problem through the established institutions and procedures of the country, would be to create by law a Code of Fair Information

Practices in the spirit of already existing legislation on labor practices. The intent of such a code would be to encourage ethical practice on the part of owners, designers, and operators of recordkeeping systems through legal deterrents. In this way it would be possible to specify how record systems should be organized and operated, how owners and operators should conduct their operations relative to the individuals about whom the information is held, what privileges and recourses the individual has, and to provide legal sanctions, both civil and criminal, that can be imposed for violations of the code.

The approach would have several advantages: It would exploit existing legal and judicial institutions and procedures. It would provide a self-adapting solution to the problem through the medium of court interpretation and judgment. It would require a minimum of new bureaucratic functions. With regard to industry, the code would be handled by the General Counsel's office, as are fair labor practices, tax matters, and other industrial regulations.

Finally, a fourth possibility is to create a Federal Record System Commission, similar to the Federal Communications Commission or the Civil Aeronautics Board, that would serve as a regulatory body to license, register, and oversee the operation of all record systems dealing with personal information. However, this would entail the creation of substantial new bureaucratic structure and funding for it. More importantly, it would also be another instance of government intervention in the affairs of the people and industry. Given our national aversion to government intervention in business and industrial activities, and the fact that deterrent mechanisms have not yet been tried, a regulatory approach to the problem of recordkeeping appears to be one that should be kept in abeyance until other methods have failed and the need for it is clearly established.

A NUMBERED SOCIETY?

The Social Security Amendments Act of 1972 (P.L. 92-603) is suggestive of what can happen if no action is taken. The Act requires that a social security number be issued to all individuals, of any age, who are receiving public assistance

from federal funds. It also authorizes, but does not require, the Secretary of Health, Education, and Welfare to take affirmative measures to assign social security numbers to all children on their initial entrance into school.

Should future legislative trend follow this precedent and gradually require all sectors of the population to have a social security number, then the United States will have reached the stage at which the population is fully numbered, a national population register can exist, and it will be technically feasible to maintain a lifetime dossier on each citizen. Other forces can lead to the same end. The introduction of the national birth certificate number will, for example, provide a unique lifetime identification for each citizen.

While a fully numbered population may not of itself be undesirable, the alarming fact is that we are drifting toward this state without public awareness that it is happening or public debate as to the possible consequences. The end result—that each of us will have a unique and permanent identifier—is not likely to happen from a well-engineered plan or deliberate intent. Rather, it will be the combined effect of many decisions, each made by someone doing his best job as he sees it at the time. It will be the cumulative effect of a variety of legislative steps, some unnoticed data collections, and a gradual widening of the operational scope of existing record systems due to economic pressures, coupled with a general ignorance that such events are occurring. In sum, a United States citizen could easily awaken one morning to find that he is uniquely identified for life and that all sorts of personal information are being collected under his label and widely disseminated for public and private use.

A NEED FOR ACTION

The issue of personal privacy has several major public-action aspects. It must be brought before the public, and kept there; the active support of consumer-oriented organizations must be solicited to promote legislative measures; public participation in the debate about a fully numbered, registered society must be encouraged.

There are also researchable aspects. One is to examine the technical details of providing comprehensive safeguards for automated information systems. Another is to analyze the legal considerations involved in protecting the individual's right to privacy. Others are a study of the consequences of a fully numbered and registered society, a search for ways to provide comprehensive protection against abuse of personal information, and the development of means for linking automated data systems while protecting the personal privacy of the data subjects.

Since automated information systems containing personal information are essential to today's complex society, it is imperative that solutions be found to the important problem of protecting our inherent right to privacy. There is certainly no question but that in the balance of power between a citizen and the totality of systems that keep records about him, he is at a significant disadvantage.