PRIVACY--HANDLING PERSONAL DATA

Willis H. Ware

October 1977

P-6042

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

PRIVACY--HANDLING PERSONAL DATA*

The present social concern commonly called privacy arises from the interplay between modern recordkeeping technology made possible largely by computer based systems and telecommunications, and the needs of modern societal institutions for information--needed to be able to function efficiently or even to function at all, and to comply with various government legislative regulations. Historically however, recordkeeping is not a new phenomenon; it has always existed. At one time however, decision-making concerning an individual was a face-to-face matter that used a record frequently jotted down as one watched. Moreover, it tended to be restricted to local use, to be stored within the organization that the individual did business with and little shared with others. Record systems were generally known to the individual and visible, but all of this is very different in the modern world. Each of us unadvoidably lives in an "information society" in which it is virtually impossible to avoid relationships with recordkeeping organizations without foregoing such necessary things as credit, insurance, medical care, education, and employment. The situation has arisen in part because society is large and mobile, in part because of a complex and affluent life style, in part because we have a service oriented culture. Thus, the small visible and local record system of yesterday has been replaced by ones that are frequently invisible, transmit information nationwide, exchange it freely with other record systems and maintain a very current data base on a huge number of individuals. The elaborate recordkeeping mechanisms of today have become a substitute for face-to-face decision making; they mediate decisions about people that are often made without human intervention.

A modern day recordkeeping system plays a gate keeping role in the sense that it very positively controls whether an individual can have access to some desired benefit, privilege, right or opportunity; in a very real way it controls the interface between an individual and the many things that society offers him. Underlying contemporary recordkeeping processes is the enormous technological component based largely on computer and telecommunications technology. The two together make possible the record systems that

---

*Published as "Handling Personal Data," Datamation, October 1977.

surround each of us, and in that sense they are the dominant driving force behind privacy questions. As professional individuals involved in such technology we therefore must be involved and responsive.

Historically, a few computer people first sounded warnings in the late 60s. Several books appeared and in 1971, the Fair Credit Reporting Act became the first legislative action. Next came the well known Secretary's Special Advisory Committee on Automated Personal Data Systems and its seminal report, "Records, Computers, and the Rights of Citizens"* which provided the intellectual basis for the Federal Privacy Act of 1974. The Act throws a broad blanket of institutional and recordkeeping behavior over Federal agencies and extends certain rights to each individual to interact with records kept about him. The Act also created the Privacy Protection Study Commission which after a two year study recently delivered its published final report.

The report of the HEW Committee spoke generally of rights for the individual and desired behavior of recordkeeping systems. It suggested that citizen and recordkeeper had a mutual interest in properly kept records; it introduced the concept of a code of Fair Information Practices. At the time privacy was seen as a matter between an individual and records that concerned him. Gradually, the issue has broadened and become better grounded; privacy is now discussed in terms of openess of recordkeeping instead of behavior of individual systems, in terms of fairness in recordkeeping instead of abuse of information or harm to the individual, in terms of an individual's expectations of confidentiality instead of a simple right to control, and in terms of social expectations rather than individual rights. The Commission, building upon the work of the HEW Committee, upon existing legislative efforts and public testimony has established its position and recommendations on the basis of three objectives which it sees as essential to an adequate public policy on privacy. In behalf of the individual, society expects

- o Creation of a proper balance between what an individual is expected to divulge to a recordkeeping system and what he seeks in return--to minimize intrusiveness.

---

*Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Department of Health, Education, and Welfare, DHEW Publication No. (OS)73-97, July 1973, available through the U. S. Government Printing Office, Stock Number 1700-00116. Also published as "Records, Computers and the Rights of Citizens," Datamation, September 1973.

- o Openess in recordkeeping operations in ways that will minimize the extent to which the record about an individual is itself a source of unfairness in any decision for which it is the basis--maximize fairness.
- o Creation and definition of obligations with respect to uses and disclosures that will be made of recorded information about an individual--create a legitmate enforceable expectation of confidentiality.

While the Commission did not attempt to create an exhaustive record of misuse of information, it nonetheless encountered such instances frequently enough to become convinced that individuals are treated unfairly through inappropriate use of records about them. The incidents sometimes represented a deliberate exploitation of systemic weaknesses in the legal environment for recordkeeping; but more often, they reflected an inconsiderate or thoughtless use of personal information or one that seemed somehow to benefit the organization--more revenue, better control, tighter decisions. In addition, because of sheer size of many modern recordkeeping systems, accuracy itself has become an important aspect of fairness. Observe for example that the Social Security Administration maintains records on approximately 200 million individuals. If only 1 percent of them contain an error and if only 1 percent of the faulty records will result in unfairness, 20,000 individuals will have been mistreated. A corresponding comment can be made about private sector systems as well. For example, a large nationwide credit reporting system will contain approximately 70 million records and using the same 1 percent and 1 percent assumptions, some 7,000 people will have been treated improperly. In such examples, it is quite clear of course how modern computer and telecommunication technology have combined to make possible and economically feasible the mammoth systems about which society has concern.

The scope of study set forth for the Commission in the Act that created it was very broad. However, the dominant task was to determine to what extent the provisions and principles of the Privacy Act of 1974 should be extended to the privacy sector. In addition, it also was to examine such collateral matters as confidentiality of Federal tax records, an individual's interaction with mailing lists, the role of Social Security numbers in recordkeeping processes, and an examination of the response and compliance

of Federal agencies with the provisions of the 1974 Act. To carry out its dominant task, the Commission held a series of public hearings over approximately 18 months and solicited testimony in such recordkeeping areas as health care, insurance, depository and lending, credit, employment, education, social assistance and research and statistics.

Because the recordkeeping practices of the private sector were largely undocumented and unknown, the Commission had no a priori position on the relevance of the Privacy Act approach to the private sector. It became convinced however, that recordkeeping in government is so different from that in the private sector and that behavior of private institutions and their managers are so diverse and differently motivated than government agencies, it would be inappropriate to create a blanket omnibus law that would spread over all of the private sector. Thus, the Commission's answer to its principal charge became: "No, the Privacy Act should not per se be extended into the public sector, but the principles and philosophy that underlie it can be." Consequently a series of approximately 165 recommendations were set forth that addressed recordkeeping practices and problems in each of the individual areas examined.

The final report of the Commission, "Personal Privacy in an Information Society"* was presented to the President and Congress on 12 July, 1977. President Carter personally expressed to the members of the Commission his intention to support its findings and stated that he would personally carry the matter to members of his Cabinet at its next meeting. During the Congressional hearing that followed the Presidential audience, it was noted that a group of bills had been introduced into the House by Representatives Koch and Goldwater to "give legislative expression" to the work of the Commission. It seems appropriate to paraphrase a well known advertisement: "We've come a long way, colleagues." In just one decade, privacy, as an evolving social issue, has moved from the warnings and cautions of a few computer people to discussion with the President--from computer conferences to the White House in ten years.

Privacy concerns are causing recordkeeping systems of all institutions of the country--public and private--to be reexamined, to be modernized and

---

* Personal Privacy in an Information Society, U.S. Government Printing Office (Superintendent of Documents, Washington, D.C. 20402), July 1977, Stock No. 052-003-00395-3.

brought into conformance with present social expectations. Record systems that have simply evolved over long periods of time will have to be changed as required. Usages of personal information that have simply happened--because of a decision that seemed right at the time--are being challenged. Interestingly, resolution of the issue interfaces with several competing societal values: first amendment interests, freedom of information interests, law enforcement interests, Federal-state relations, and cost of privacy safeguards.

The general thrust of the Commission recommendations is openness and fairness in recordkeeping. As an individual establishes a relation with a private sector recordkeeping organization, he will be fully informed about such things as: what records will be kept about him, what information will be collected, what role his records will play in decisions about him, with what organizations the record will be shared, by what organizations the record or portions of it will be verified, his right to see and copy and correct the record, and an assurance that his records will be protected as confidential information. From such a broad position flows a whole series of detailed recommendations that are intended to be implemented in part by new Federal law, in part by amended Federal law, in part by new state law, and in part by voluntary compliance. No new regulatory bodies are required; existing ones at Federal or state level are sufficient. The detailed recommendations are a blend of fair information practices, limits on collection, limits on disclosure, propagation of corrections, a restriction on the use of some items for decision-making, a separation between certain types of records on the same individual, an emphasis on accuracy of recordkeeping, control of access on a strict need-to-know basis, disclosure of only the pertinent portion of the record for a stated purpose, plus a number of behavioral constraints levied on the institution per se rather than on its recordkeeping system, e.g., to exercise due care in the selection of investigative organizations, to not collect information under false pretense or pretext. Throughout of course are many implications for design or redesign of computer-based as well as manual recordkeeping systems. What are some of these?

In all areas examined, the individual is to be given a legally enforceable expectation of confidentiality in regard to his records. This implies of course that personal information must be protected against

inadvertent disclosure and it also implies that access to it by third parties must be carefully controlled. It also implies that access to it by authorized individuals must be on a strict need-to-know basis, that the uses to which the information can be put by such individuals must be carefully specified by the corporate structure and that employees must be monitored for compliance and disciplined when necessary. In each area studied, the individual is given the right to see-and-copy his record and to cause errors that he has noticed to be corrected.* A recordkeeping system therefore must be prepared to mark any items in the record which are disputed so that any disclosure to other parties will be appropriately flagged or not disclosed. In case a dispute cannot be resolved, then the record system must be prepared to accept a short statement of the individual's side of the matter. If a data base supports a number of diverse recordkeeping functions, then the system must be prepared to divulge to the individual only that portion of the record which he has currently asked to see. It goes without saying of course that computerized systems must be prepared to show information to people in a form that is understandable and must either be prepared to provide copies upon request, or to allow any individual to make his own.

If an individual discovers an error, then the recordkeeping institution is required to propagate the correction to recipients of the record and in some cases will also be required to propagate a correction backward to the source of the error. Since the Commission dealt with communities of recordkeeping (e.g., insurance companies plus their insurance support organizations plus the Medical Information Bureau), the intent is that propagation of corrections will automatically take place as required throughout whatever community normally interacts as a matter of business; but in addition, the individual may request that a correction be forwarded to a specific organization(s) that he names. Authorizations signed by an individual for release of information about him are to be specific as to organization to be contacted, information to be solicited, purpose for which to be used, and calendar period over which the authorization remains valid. Thus, a recordkeeping system must be prepared to disclose to third parties only that portion of the record which is pertinent to the authorized request or to the purpose intended.

---

*This is in distinction to the Fair Credit Reporting Act that provides "an individual is to be told the nature and substance" of the record.

In such areas as insurance or consumer credit, if an individual receives an adverse decision, he is to be told exactly what items in the record have resulted in the decision. Again, a recordkeeping system must be prepared to disclose portions of the record on a selective basis. In the same two areas, the Commission has recommended that a government mechanism should exist whereby individuals can question the propriety of collecting and/or using certain items of information.* Thus, a record-keeping system would have to distinguish between information that it collects for auditing or compliance purposes and information that is permitted to be used for decision-making about people.

In the employment and personnel area where compliance is voluntary, it is recommended that management take affirmative action to review all such records and to purge them of information not relevant or no longer necessary. Moreover, it is also recommended in employment and also in education that certain records not be commingled, e.g., security records are to be kept separate from personnel records, law enforcement investigations are to be kept separate from education records. Thus, either separated recordkeeping systems must exist in such instances, or mechanisms must exist to assure access only by relevant users.

In addition to the technical consequences, there are of course also management, administrative and procedural ones. There will have to be affirmative actions to acquaint users of personal information with limitations imposed on it, with disiplinary actions to be invoked in case of misbehavior, and with the legal consequences of breach of confidentiality. Management will also have to create procedures to comply with the recommendation that information not be available to third parties without consent of the individual except by formal judicial process. Thus, employees will have to be informed on the proper response to a subpoena. Management will also have to institute procedures to ensure that records about people are maintained with accuracy, timeliness and completeness. It will also have to avoid certain types of information collection, such as by polygraph or by pretext interviews. Under certain circumstances a procedure will be required to obtain the consent of an individual before using information about

---

*For example, the Commissioner of Insurance in California has ruled that sexual preference and life style information may not be used in making insurance decisions although it may be collected.

him for a different purpose. Finally, of course, there will be a one time task of deciding what response is relevant to such privacy legislation as might be passed and of bringing the corporate body of recordkeeping systems into compliance with them.

Ultimately of course, data processing people will have to decide what technical safeguards--and perhaps procedural ones as well--should be put in place. Privacy law will inevitably speak generally and establish broad social goals; therefore, it will not be in the nature of tight technical specifications to which the computer person is accustomed to respond. Thus, the corporate management must establish the general guidance and determine the organization's broad response. Management cannot abdicate its responsibility for interpreting the intent of the legislative process to its data processing group, although the latter clearly has an essential role in helping management converge to an appropriate posture. Civil and criminal penalties that will be a part of privacy legislation will fall upon the organization; therefore, its management must take the lead in providing adequate direction to its computer people and recordkeeping specialists.

The technical consequences outlined above are illustrative and fairly obvious ones; in the long run, there are more subtle ones. The trend is obviously toward functionally integrated data bases in which "the record" about any individual will contain everything an organization knows about him. Only portions of the record however are authorized to various individuals; and thus, access control on a finer grain than to the entire record will become necessary; it may be required to control the data element level. There is an increasingly important issue of granularity that will characterize future recordkeeping systems. To some extent it is already upon us, but in many instances it has been circumvented by maintaining separate data bases in support of different record systems.

Of increasing importance also is so-called "descriptor-data" that tells something either about a data element or about the structure of data. For example, in contemporary record systems for consumer credit, a charge in dispute has to be flagged so that interest is not levied against it until the uncertainty is resolved. In view of the right that an individual will have under privacy legislation to contest items in the record, it will probably be of increasing importance that disputed items are either not disclosed only with a disputed notation accompanying them, or excluded from

certain decision-making activities. When the matter is finally resolved, there is likely to be retroactive actions to restore the record, or reverse decisions, or take administrative action. Thus, a comprehensive integrated record system of the future will have to incorporate various kinds of descriptor-data within the record in order to cue the system to treat various items of information in special ways at special times, or to guide the system in selectively disclosing information to authorized recipients or authorized third parties of various kinds.

Since accuracy is an underlying tenant of fairness in recordkeeping, there are numerous Commission recommendations for the propagation of corrections, both forward to recipients of an erroneous record and backward to sources of erroneous data. Thus, a record must include such supplementary data as is needed in order to be able to reconstruct as required the trail from data sources or to record recipients. Such "traffic data" will be essential if the technical impact of propagating corrections is to be minimized. Notice also that technical details such as just suggested are matters for not only the record system that discloses, but also for the one that receives records from others. Both must be able to deal properly with descriptor-data and with traffic data.

As a final observation, lest anyone believe that an appropriate response to privacy legislation must await the creating of foolproof computer security safeguards, it is to be noted that the threat against personal information is not the dishonest person seeking to steal or pirate information about someone, but rather is the honest individual doing his authorized job, but not realizing that certain things which he does with personal information or certain ways in which he uses it is to the disinterest or disadvantage of an individual concerned--actions perhaps because the organization has failed to guide him properly. Thus, the computer security problem in regard to privacy is more one of sound information practices than it is one of provable security kernels and operating systems guaranteed free of loopholes. An adequate response to such privacy legislation as may materialize in the coming year certainly need not await the solution of several difficult research problems now being pursued in the name of computer security.

Data processing professionals involved with recordkeeping systems have an exciting several years ahead as the public and private institutions of

the country bring their systems into conformance with modern day attitudes toward the use of information about people. Managements also have their period of trial in which they interpret as best they can what the thrust and intent of privacy legislation is, and wait out the gradual accumulation of case law that ultimately gives interpretation and detail to a law. In spite of whatever difficulty may exist ahead, progress is essential both for the welfare of our society and the preservation of our personal freedoms as we want them to be. The ease with which information can now be automatically captured, stored, or disseminated and with which it can migrate from place to place simply is too large a threat of many dimensions to the individual. Some level of legal control and oversight is a must.