RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS

Willis H. Ware

August 1973

P-5077

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

RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS*

W. H. Ware
The Rand Corporation, Santa Monica, California

In early 1972, then Secretary of Health, Education and Welfare Elliot Richardson, created a Special Advisory Committee with the charge to analyze harmful consequences that might result from automated personal data systems, and to make recommendations about safeguards that might protect individuals against potentially harmful consequences and afford them redress for any harm. Since the Social Security Number has been widely used as a personal identifier, the Committee was also asked to examine the policy and practice relating to the issuance and use of such numbers. On July 31, 1973, the Committee submitted its final report to now Secretary of Health, Education and Welfare Caspar Weinberger, with Attorney General Elliot Richardson in attendance.

As a document intended for busy government officials, this report included a summary of its findings in the early pages. In addition, the press conference at which it was released briefly summarized its findings and recommendations; and as one might expect, the initial press coverage and reporting highlighted the committee recommendations rather than giving a careful exposition of the rationale by which the position had been reached. To put the findings of this committee in perspective and proper context, the following discussion draws on selected segments of the report.

---

*"Records, Computers and the Rights of Citizens", Report of the Secretary's Advisory Committee on Automated Personal Data Systems, DHEW Publication Number (OS)73-94, Government Printing Office Stock No. 1700-00116, Superintendent of Documents, U.S. Government Printing Office, Washington, D. C. 20402

The central issue of concern is the record-keeping practices of the government and private agencies that deal with personal information about people. While not all such records are maintained by computer, those that are become of especial concern because the concentration of information within computer files at one location and the access to such files through remote access terminals tend to magnify the opportunities for misuse of personal information. Relative to the totality of the record-keeping systems that surround each of us today, any one individual finds himself at a significant disadvantage to affect the content of the records or to limit their usage. Most of us have suffered at least the annoyance of having to cope with a computer-based system that, outwardly at least, appears not to care how it has mistreated us or, worse, has given false impression or subjected us to harrassment. It is, of course, true that the computer per se is not the culprit; rather the system designers have, for whatever reasons, seen fit not to create humane systems that are considerate of the data subjects about whom information is held. Thus, in the struggle to protect the personal privacy of the citizen, the preferred solution would adjust the balance of power between citizen and record system in such fashion that the individual has both opportunity and a mechanism to contest, correct and control personal information held about himself.

It is helpful to review suggestions that have been made to deal with the matter of protecting data subjects against harm. One proposal has been to license and certify computer programmers and systems designers with the hope that such a procedure would improve the care with which record-keeping systems are designed and operated. While assuredly useful, it cannot of itself adequately protect data subjects against potential harm. The best designed system in the world cannot prevent

authorized users of the system from maliciously using the information. More to the point, however, a certification approach would put the responsibility for a properly designed and controlled record system in the wrong place. The responsibility should be upon the organization that assembles the system, initiates its design and operates it, not upon the technical professionals who implement it.

A second suggestion is the ombudsman approach that 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 a bureaucracy in matters of dispute. While the concept is a useful third-party mechanism to facilitate resolution of an argument, it is not well established in this country nor is it a sufficiently broad and powerful force to bring about essential changes in how record-keeping systems are designed and deterred from inappropriate behavior.

There have been many definitions of privacy [Ibid pg. 39] all of which contain the common element that personal data are bound to be disclosed and that the data subject should have some hand in deciding the nature and extent of such disclosure. As the Committee phrased it, "personal privacy as it relates to personal-data record-keeping must be understood in terms of a concept of mutuality". The organization that holds personal data must not have complete control over it and, conversely, neither may the data subject. Each has a stake in seeing that the information is used properly. As part of the Committee's definition of privacy, it was suggested that, "a record containing information about an individual in identifiable form must...be governed by procedures that afford the individual a right to participate in deciding

what the content of the record will be and what disclosure and use will be made of the identifiable information in it. Any recording, disclosure and use of identifiable personal information not governed by such procedures must be proscribed as an unfair information practice unless such recording, disclosure or use is specifically authorized by law".

Thus, the Committee concluded that safeguards for personal privacy based on such a concept of mutuality in record-keeping requires adherence by record-keeping organizations to certain fundamental principles which collectively define a principle of *fair information practice*. We propose [Ibid pg. 41] that

- there must be no personal-data record-keeping systems whose very existence is secret,
- there must be a way for an individual to find out what information about him is in the record and how it is used,
- there must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent,
- there must be a way for an individual to correct or amend a record of identifiable information about him, and
- any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precaution to prevent misuse of the data.

The principles just given are considered by the Committee as the minimum set of rights that should be available to the individual. The question becomes how to extend these rights to the citizen. An obvious

mechanism, and one that has been suggested many times, is the creation of a centralized federal agency to regulate all automated personal data systems. Such an agency would be expected to register or license the operation of such systems, could establish specific safeguards as a condition of registration or licensure and would generally be the watchdog over all data banks public and private. Because systems used by the enormous number and variety of institutions dealing with personal data vary greatly in purpose, complexity, scope and administrative context, an agency to regulate, license and control such a breadth of activity would have to be both large in scale and pervasive. The procedures for regulation or licensing would become extremely complicated, costly, and might unnecessarily interfere with desirable application of computers to record keeping. Moreover, such a regulatory body would be another instance of federal government intrusion into the affairs of industry, the citizen, and other levels of government.

Thus, the Committee has proposed a solution that was felt to provide for the citizen equally strong rights but at the same time to avoid the necessity for a regulatory body. It has recommended that there be created by legislation a Code of Fair Information Practice applicable to all automated personal data systems [Ibid pg. 50]. This Code would define "fair information practice" as adherence to specified safeguard requirements, would prohibit violation of any requirement as an unfair information practice, would provide both civil and criminal penalties for unfair information practice, would provide for injunctions to prevent violation of any safeguard requirements and, finally, would permit both individual and class actionable suits for actual liquidated and punitive damages. This approach, the Committee is convinced, would not impose

constraints on the application of electronic data processing technology beyond those necessary to assure the maintenance of reasonable standards of personal privacy in record keeping. It would imply no new federal bureaucracy and should be inexpensive of enforcement at government level. Importantly, this approach exploits the established legal and judicial institutions and practices of the country and, through court decisions and judgements, can provide an adaptable solution that reflects shifts in the attitudes of society. From the standpoint of industry, the monitoring of fair information practice would become a matter for the General Counsel's office as he is already concerned with fair labor practice and other requirements levied by law.

We were led to this concept by noting that organizations operating personal automated data systems should be *deterred* from inappropriate practices rather than being forced by regulation to adopt specific practices. The most universal deterrent seems to be financial and thus we structured our code and its safeguards in terms of financial penalties; this is already the case for many other damage-recovery procedures under law.

To implement such a Fair Information Practices Code we suggest certain safeguard requirements [Ibid pg. 53 ff.]. One set stipulates that any organization maintaining an administrative personal data system

- shall identify one person immediately responsible for the system,
- shall take affirmative action to inform each of its employees about the safeguard requirements and rules and procedures governing the conduct of the system,
- shall specify penalties to be applied to any employees who violate the safeguard,
- shall take reasonable precautions to protect data in the system from anticipated threats

or hazards to the security of the system,

- shall make no transfer of identifiable personal data to another system unless such other system also fulfills the safeguard requirements, etc.

A second set deals with the public notice requirement and stipulates that any organization maintaining an administrative automated personal data system must give public notice of the existence and character of the system once each year. Furthermore, any organization "proposing to establish a new system or to enlarge an existing system shall give public notice long enough in advance... to assure individuals who may be affected by its operation a reasonable opportunity to comment".

Finally, a third set stipulates the rights of individual data subjects and includes such things as any organization maintaining an administrative automated personal data system

- shall inform an individual when asked to supply personal data whether he is legally required or may refuse to supply the data requested,
- shall inform an individual upon request whether he is the subject of data in the system and, if so, make such data fully available to him,
- shall assure that no use of individually identifiable data is made that is not within the stated purposes of the system,
- shall inform an individual upon request about the uses made of data about him including the identity of all persons and organizations involved and their relations with the system,
- shall assure that no data about an individual are made available in response to a demand for data by means of compulsory legal process

unless the individual to whom the data pertains has been notified of the demand, and

- shall maintain procedures that allow an individual who is the subject of data in the system to contest their accuracy, completeness, pertinence, and the necessity for retaining them, that permit data to be corrected or amended when the individual so requests, and assure when there is disagreement that the individual's claim is noted and included in any subsequent disclosure or dissemination of the disputed data.

We regard the safeguards just outlined as a minimum set. Whether they are exactly the proper set, of course, can be debated. The important point is that a Code of Fair Information Practice defined in terms of certain safeguards is a viable and, so far as can now be seen, adequate solution to the problem of protecting personal privacy.

Systems that maintain personal data in identifiable form are also used for statistical reporting and research. In such applications, the identification is usually stripped from the data and aggregated or statistical assessments made. There are other systems, usually called statistical-reporting and research systems, that never deal with identifiable data. For each of these, the appropriate set of safeguards is slightly different but, in general, act to the same end [Ibid; Chapter 5, pg. 78 ff., and Chapter 6, pg. 89 ff.]

The second major issue to be considered by the Committee was that of the Social Security Number and its growing status as a standard universal identifier. The initial press reporting of our report stated simply that we were against the use of the Social Security Number as a personal identifier but excluded the supporting arguments.

The Committee included both data processing experts and a number of individuals each responsible for the operation of large record-keeping systems. It was certainly understood by all that a standard universal identifier that could be assigned to an individual for his lifetime has positive value. Our argument against the use of the Social Security Number rests partly on the fact that the Social Security Number is not a good candidate for a standard universal identifier [Ibid; pp. 112-114]. For example, the Social Security Administration estimates that more than 4.2 million people have two or more Social Security Numbers; thus, the SSN is not adequately unique. Furthermore, the SSN has no check feature and most randomly chosen nine-digit numbers cannot be distinguished from a valid SSN. For these and other reasons the Social Security Number is not adequately reliable as a standard universal identifier.

There is a much more important aspect than the shortcomings of the Social Security Number as a potential de facto standard universal identifier. There has not yet been a public debate on the issue of a personal identifier nor has there been an assessment of the social consequences. Moreover, there are inadequate legal and social safeguards against abuse of personal information contained in automated personal data systems. In view of these facts, we take the position that "a standard universal identifier should not be established in the United States now or in the foreseeable future". However, we acknowledge that a standard universal identifier does have positive social value in some circumstances and we would urge that the question surely be reexamined when adequate legal and social safeguards have been established and shown effective in protecting the personal privacy of the individual citizen.

Meanwhile, in order to constrain the spread of the Social Security Number as a de facto standard identifier, we recommend that

- o uses of the Social Security Number be limited to those necessary for carrying out requirements imposed by the federal government, and
- o that federal agencies and departments should not require nor promote use of the Social Security Number except to the extent that they have specific legislation mandated from the Congress to do so.

To further restrict the spread of the Social Security Number in its identifier role, we recommend [Ibid pg. 125 ff.] that legislation be passed that

- o gives the individual a legal right to refuse to disclose his Social Security Number to any person or organization that does not have specific federal authority to request it,
- o provides that an individual have the right to redress if his lawful refusal to disclose his Social Security Number results in the denial of a benefit or the threat of denial of a benefit and,
- o requires any oral or written request made to an individual for his Social Security Number be accompanied by a clear statement indicating whether or not compliance with the request is required by federal statute and, if so, citing the specific legal requirement.

We have also made a number of other recommendations with regard to the Social Security Number, the net effect of which is to restrict its use to those purposes mandated by federal law, to urge the Social Security Administration not to assign Social Security Numbers to children below ninth grade level and to give the Social Security Number the status of a confidential item of information.

In the struggle to assure and protect the privacy of the individual and to afford him redress against any harm that might befall him through the operation of an automated personal data system, we are convinced that adequate deterrents against abuse of personal information can be provided through the mechanism of a Code for Fair Information Practice. We believe that a regulatory approach is neither necessary nor desirable. With regard to the role that the Social Security Number plays in the dissemination of personal information and the linking of items of personal information coming from different sources, we are convinced that the American public has not yet adequately considered the implication of a standard universal lifetime identifier and we, therefore, take the position that until such conscious debate has occurred and until adequate social and legal safeguards against abuse of personal information exist and have been shown to be effective, the Social Security Number should be tightly constrained as to its use.