Summary and Recommendations

The Secretary’s Advisory Committee on Automated Personal Data Systems comprised a cross section of experienced and concerned citizens appointed by the Secretary of Health, Education, and Welfare to analyze the consequences of using computers to keep records about people. The Committee assessed the impact of computer-based record keeping on private and public matters and recommended safeguards against its potentially adverse effects. The Committee paid particular attention to the dangers implicit in the drift of the Social Security number toward becoming an all-purpose personal identifier and examined the need to insulate statistical-reporting and research data from compulsory legal process.

The Committee’s report begins with a brief review of the historical development of records and record keeping, noting the different origins of administrative, statistical, and intelligence records, and the different traditions and practices that have grown up around them. It observes that the application of computers to record keeping has challenged traditional constraints on record-keeping practices. The computer enables organizations to enlarge their data-processing capacity substantially, while greatly facilitating access to recorded data, both within organizations and across boundaries that separate them. In addition, computerization creates a new class of record keepers whose functions are technical and whose contact with the suppliers and users of data are often remote.
The report explores some of the consequences of these changes and assesses their potential for adverse effect on individuals, organizations, and the society as a whole. It concludes that the net effect of computerization is that it is becoming much easier for record-keeping systems to affect people than for people to affect record-keeping systems. Even in non-governmental settings, an individual's control over the use that is made of personal data he gives to an organization, or that an organization obtains about him, is lessening.

Concern about computer-based record keeping usually centers on its implications for personal privacy, and understandably so if privacy is considered to entail control by an individual over the uses made of information about him. In many circumstances in modern life, an individual must either surrender some of that control or forego the services that an organization provides. Although there is nothing inherently unfair in trading some measure of privacy for a benefit, both parties to the exchange should participate in setting the terms.

Under current law, a person's privacy is poorly protected against arbitrary or abusive record-keeping practices. For this reason, as well as because of the need to establish standards of record-keeping practice appropriate to the computer age, the report recommends the enactment of a Federal "Code of Fair Information Practice" for all automated personal data systems. The Code rests on five basic principles that would be given legal effect as "safeguard requirements" for automated personal data systems.

- 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 a record and how it is used.
- There must be a way for an individual to prevent information about him that was 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.

- 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 precautions to prevent misuse of the data.

The proposed Code calls for two sets of safeguard requirements; one for administrative automated personal data systems and the other for automated personal data systems used exclusively for statistical reporting and research. Special safeguards are recommended for administrative personal data systems whose statistical-reporting and research applications are used to influence public policy.

The safeguard requirements define minimum standards of fair information practice. Under the proposed Code, violation of any safeguard requirement would constitute "unfair information practice" subject to criminal penalties and civil remedies. The Code would also provide for injunctive relief. Pending legislative enactment of such a code, the report recommends that the safeguard requirements be applied through Federal administrative action.

The report discusses the relationship of existing law to the proposed safeguard requirements. It recommends that laws that do not meet the standards set by the safeguard requirements for administrative personal data systems be amended and that legislation be enacted to protect personal data used for statistical reporting and research from compulsory disclosure in identifiable form.

The report examines the characteristics and implications of a standard universal identifier and opposes the establishment of such an identification scheme at this time. After reviewing the drift toward using the Social Security number (SSN) as a de facto standard universal identifier, the Committee recommends steps to curtail that drift. A persistent source of public concern is that the Social Security number will be used to assemble dossiers on individuals from fragments of data in widely dispersed systems. Although this is a more difficult technical feat than most laymen realize, the increasing use of the Social Security number to distinguish among individuals with the same name, and to match
RECOMMENDATIONS

Code of Fair Information Practice

We recommend the enactment of legislation establishing a Code of Fair Information practice for all automated personal data systems.

- The Code should define "fair information practice" as adherence to specified safeguard requirements.
- The Code should prohibit violation of any safeguard requirement as an "unfair information practice."
- The Code should provide that an unfair information practice be subject to both civil and criminal penalties.
- The Code should provide for injunctions to prevent violation of any safeguard requirement.
- The Code should give individuals the right to bring suits for unfair information practices to recover actual, liquidated, and punitive damages, in individual or class actions. It should also provide for recovery of reasonable attorneys' fees and other costs of litigation incurred by individuals who bring successful suits.

Pending the enactment of a code of fair information practice, we recommend that all Federal agencies (i) apply the safeguard requirements, by administrative action, to all Federal systems, and (ii) assure, through formal rule making, that the safeguard requirements are applied to all other systems within reach of the Federal government's authority. Pending the enactment of a code of fair information practice, we urge that State and local governments, the institutions within reach of their authority, and all private organizations adopt the safeguard requirements by whatever means are appropriate.
Safeguards Requirements for
Administrative Personal Data Systems

I. GENERAL REQUIREMENTS

A. Any organization maintaining a record of individually identifiable personal data, which it does not maintain as part of an administrative automated personal data system, shall make no transfer of any such data to another organization, without the prior informed consent of the individual to whom the data pertain; if, as a consequence of the transfer, such data will become part of an administrative automated personal data system that is not subject to these safeguard requirements.

B. Any organization maintaining an administrative automated personal data system shall:

1. Identify one person immediately responsible for the system, and make any other organizational arrangements that are necessary to assure continuing attention to the fulfillment of the safeguard requirements;

2. Take affirmative action to inform each of its employees having any responsibility or function in the design, development, operation, or maintenance of the system, or the use of any data contained therein, about all the safeguard requirements and all the rules and procedures of the organization designed to assure compliance with them;

3. Specify penalties to be applied to any employee who initiates or otherwise contributes to any disciplinary or other punitive action against any individual who brings to the attention of appropriate authorities, the press, or any member of the public, evidence of unfair information practice;

4. Take reasonable precautions to protect data in the system from any anticipated threats or hazards to the security of the system;

5. Make no transfer of individually identifiable personal data to another system without (i) specifying requirements for security of the data, including limitations on access thereto, and (ii) determining that the conditions of the transfer provide substantial assurance that those requirements and limitations will be observed—except in instances when an individual specifically requests that data about him be transferred to another system or organization;

6. Maintain a complete and accurate record of every access to and use made of any data in the system, including the identity of all persons and organizations to which access has been given;

7. Maintain data in the system with such accuracy, completeness, timeliness, and pertinence as is necessary to assure accuracy and fairness in any determination relating to an individual’s qualifications, character, rights, opportunities, or benefits, that may be made on the basis of such data; and

8. Eliminate data from computer-accessible files when the data are no longer timely.

II. PUBLIC NOTICE REQUIREMENT

Any organization maintaining an administrative automated personal data system shall give public notice of the existence and character of its system once each year. Any organization maintaining more than one system shall publish such annual notices for all its systems simultaneously. Any organization proposing to establish a new system, or to enlarge an existing system, shall give public notice long enough in advance of the initiation or enlargement of the system to assure individuals who may be affected by its operation a reasonable opportunity to comment. The public notice shall specify:

1. The name of the system;

2. The nature and purpose(s) of the system;

3. The categories and number of persons on whom data are (to be) maintained;

4. The categories of data (to be) maintained, indicating which categories are (to be) stored in computer-accessible files;

5. The organization’s policies and practices regarding data storage, duration of retention of data, and disposal thereof;

6. The categories of data sources;

7. A description of all types of use (to be) made of data, indicating those involving computer-accessible files, and including all classes of users and the organizational relationships among them;

8. The procedures whereby an individual can (i) be informed if he is the subject of data in the system; (ii) gain access to such data; and (iii) contest their accuracy, completeness, pertinence, and the necessity for retaining them;
(9) The title, name, and address of the person immediately responsible for the system.

III. RIGHTS OF INDIVIDUAL DATA SUBJECTS

Any organization maintaining an administrative automated personal data system shall:

(1) Inform an individual asked to supply personal data for the system whether he is legally required, or may refuse, to supply the data requested, and also of any specific consequences for him, which are known to the organization, of providing or not providing such data;

(2) Inform an individual, upon his request, whether he is the subject of data in the system, and, if so, make such data fully available to the individual, upon his request, in a form comprehensible to him;

(3) Assure that no use of individually identifiable data is made that is not within the stated purposes of the system as reasonably understood by the individual, unless the informed consent of the individual has been explicitly obtained;

(4) Inform an individual, upon his request, about the uses made of data about him, including the identity of all persons and organizations involved and their relationships with the system;

(5) Assure that no data about an individual are made available from the system in response to a demand for data made by means of compulsory legal process, unless the individual to whom the data pertain has been notified of the demand; and

(6) Maintain procedures that (i) allow an individual who is the subject of data in the system to contest their accuracy, completeness, pertinence, and the necessity for retaining them; (ii) permit data to be corrected or amended when the individual to whom they pertain so requests; and (iii) assure, when there is disagreement with the individual about whether a correction or amendment should be made, that the individual's claim is noted and included in any subsequent disclosure or dissemination of the disputed data.

Summary and Recommendations

Existing laws or regulations affording individuals greater protection than the safeguard requirements should be retained, and those providing less protection should be amended to meet the basic standards set by the safeguards. In particular, we recommend:

- That the Freedom of Information Act be amended to require an agency to obtain the consent of an individual before disclosing in personally identifiable form exempted-category data about him, unless the disclosure is within the purposes of the system as specifically required by statute.

- That pending such amendment of the Act, all Federal agencies provide for obtaining the consent of individuals before disclosing individually identifiable exempted-category data about them under the Freedom of Information Act.

- That the Fair Credit Reporting Act be amended to provide for actual, personal inspection by an individual of his record along with the opportunity to copy its contents, or to have copies made; and that the exceptions from disclosure to the individual now authorized by the Fair Credit Reporting Act for medical information and sources of investigative information be omitted.

Statistical-Reporting and Research Uses of Administrative Personal Data Systems

In light of our inquiry into the statistical-reporting and research uses of personal data in administrative record-keeping systems, we recommend that steps be taken to assure that all such uses are carried out in accordance with five principles:

First, when personal data are collected for administrative purposes, individuals should under no circumstances be coerced into providing additional personal data that are to be used exclusively for statistical reporting and research. When application forms or other means of collecting personal data for an administrative data system are designed, the mandatory or voluntary character of an individual's responses should be made clear.
Second, personal data used for making determinations about an individual's character, qualifications, rights, benefits, or opportunities, and personal data collected and used for statistical reporting and research, should be processed and stored separately.

Third, the amount of supplementary statistical-reporting and research data collected and stored in personally identifiable form should be kept to a minimum.

Fourth, proposals to use administrative records for statistical reporting and research should be subjected to careful scrutiny by persons of strong statistical and research competence.

Fifth, any published findings or reports that result from secondary statistical-reporting and research uses of administrative personal data systems should meet the highest standards of error measurement and documentation.

In addition, there are certain safeguards that can be feasibly applied to all administrative personal data systems used for statistical reporting and research. Specifically, we recommend that the following requirements be added to the safeguard requirements for administrative personal data systems:

- Under I. General Requirements, add—

  C. Any organization maintaining an administrative automated personal data system that publicly disseminates statistical reports or research findings based on personal data drawn from the system, or from systems of other organizations, shall:

  (1) Make such data publicly available for independent analysis, on reasonable terms; and

  (2) Take reasonable precautions to assure that no data made available for independent analysis will be used in a way that might reasonably be expected to prejudice judgments about any individual data subject's character, qualifications, rights, opportunities, or benefits.

- Under the Public Notice Requirement, add—

  (8a) The procedures whereby an individual, group, or organization can gain access to data used for statistical reporting or research in order to subject such data to independent analysis.

Systems Used Exclusively for Statistical Reporting and Research

All the features of the Code of Fair Information Practice that we recommend for automated personal data systems would apply to systems used exclusively for statistical reporting and research. The safeguard requirements to be included in the Code for such systems are designed to help protect the individual citizen against unintended or unforeseen uses of information that he provides exclusively for statistical reporting and research, and to help assure that the uses organizations make of such data are subject to independent expert review and open public discussion. Pending the enactment of a code of fair information practice, we also urge that State and local governments, the institutions within reach of their authority, and all private organizations adopt the safeguard requirements by whatever means are appropriate.

Safeguard Requirements for Statistical-Reporting and Research Systems

I. GENERAL REQUIREMENTS

A. Any organization maintaining a record of personal data, which it does not maintain as part of an automated personal data system used exclusively for statistical reporting or research, shall make no transfer of any such data to another organization without the prior informed consent of the individual to whom the data pertain, if, as a consequence of the transfer, such data will become part of an automated personal data system that is not subject to these safeguard requirements or the safeguard requirements for administrative personal data systems.
B. Any organization maintaining an automated personal data system used exclusively for statistical reporting or research shall:

1. Identify one person immediately responsible for the system, and make any other organizational arrangements that are necessary to assure continuing attention to the fulfillment of the safeguard requirements;

2. Take affirmative action to inform each of its employees having any responsibility or function in the design, development, operation, or maintenance of the system, or the use of any data contained therein, about all the safeguard requirements and all the rules and procedures of the organization designed to assure compliance with them;

3. Specify penalties to be applied to any employee who initiates or otherwise contributes to any disciplinary or other punitive action against any individual who brings to the attention of appropriate authorities, the press, or any member of the public, evidence of unfair information practice;

4. Take reasonable precautions to protect data in the system from any anticipated threats or hazards to the security of the system;

5. Make no transfer of individually identifiable personal data to another system without (i) specifying requirements for security of the data, including limitations on access thereto, and (ii) determining that the conditions of the transfer provide substantial assurance that those requirements and limitations will be observed—except in instances when each of the individuals about whom data are to be transferred has given his prior informed consent to the transfer; and

6. Have the capacity to make fully documented data readily available for independent analysis.

II. PUBLIC NOTICE REQUIREMENT

Any organization maintaining an automated personal data system used exclusively for statistical reporting or research shall give public notice of the existence and character of its system once each year. Any organization maintaining more than one such system shall publish annual notices for all its systems simultaneously. Any organization proposing to establish a new system, or to enlarge an existing system, shall give public notice long enough in advance of the initiation or enlargement of the system to assure individuals who may be affected by its operation a reasonable opportunity to comment. The public notice shall specify:

Summary and Recommendations

1. The name of the system;

2. The nature and purpose(s) of the system;

3. The categories and number of persons on whom data are (to be) maintained;

4. The categories of data (to be) maintained, indicating which categories are (to be) stored in computer-accessible files;

5. The organization's policies and practices regarding data storage, duration of retention of data, and disposal thereof;

6. The categories of data sources;

7. A description of all types of use (to be) made of data, indicating those involving computer-accessible files, and including all classes of users and the organizational relationships among them;

8. The procedures whereby an individual, group, or organization can gain access to data for independent analysis;

9. The title, name, and address of the person immediately responsible for the system;

10. A statement of the system's provisions for data confidentiality and the legal basis for them.

III. RIGHTS OF INDIVIDUAL DATA SUBJECTS

Any organization maintaining an automated personal data system used exclusively for statistical reporting or research shall:

1. Inform an individual asked to supply personal data for the system whether he is legally required, or may refuse, to supply the data requested, and also of any specific consequences for him which are known to the organization, of providing or not providing such data;

2. Assure that no use of individually identifiable data is made that is not within the stated purposes of the system as reasonably understood by the individual, unless the informed consent of the individual has been explicitly obtained;

3. Assure that no data about an individual are made available from the system in response to a demand for data made by means of compulsory legal process, unless the individual to whom the data pertain (i) has been notified of the demand, and (ii) has been afforded full access to the data before they are made available in response to the demand.
In addition to the foregoing safeguard requirements for all automated personal data systems used exclusively for statistical reporting and research, we recommend that all personal data in such systems be protected by statute from compulsory disclosure in identifiable form. Federal legislation protecting against compulsory disclosure should include the following features:

- The data to be protected should be limited to those used exclusively for statistical reporting or research. Thus, the protection would apply to statistical-reporting and research data derived from administrative records, and kept apart from them, but not to the administrative records themselves.
- The protection should be limited to data identifiable with, or traceable to, specific individuals. When data are released in statistical form, reasonable precautions to protect against "statistical disclosure" should be considered to fulfill the obligation to disclose data that can be traced to specific individuals.
- The protection should be specific enough to qualify for non-disclosure under the Freedom of Information Act exemption for matters "specifically exempted from disclosure by statute." 5 U.S.C. 552(b)(3).
- The protection should be available for data in the custody of all statistical-reporting and research systems, whether supported by Federal funds or not.
- Either the data custodian or the individual about whom data are sought by legal process should be able to invoke the protection, but only the individual should be able to waive it.
- The Federal law should be controlling; no State statute should be taken to interfere with the protection it provides.

Use of the Social Security Number

We take the position that a standard universal identifier (SUI) should not be established in the United States now or in the foreseeable future. By our definition, the Social Security Number (SSN) cannot fully qualify as an SUI; it only approximates one. However, there is an increasing tendency for the Social Security number to be used as if it were an SUI. There are pressures on the Social Security Administration to do things that make the SSN more nearly an SUI.

We believe that any action that would tend to make the SSN more nearly an SUI should be taken only if, after careful deliberation, it appears justifiable and any attendant risks can be avoided. We recommend against the adoption of any nationwide, standard, personal identification format, with or without the SSN, that would enhance the likelihood of arbitrary or uncontrolled linkage of records about people, particularly between government and government-supported automated personal data systems.

We believe that until safeguards against abuse of automated personal data systems have become effective, constraints should be imposed on use of the Social Security number. After that the question of SSN use might properly be reopened.

As a general framework for action on the Social Security number, we recommend that Federal policy with respect to use of the SSN be governed by the following principles:

First, use of the SSN should be limited to those necessary for carrying out requirements imposed by the Federal government.

Second, Federal agencies and departments should not require or promote use of the SSN except to the extent that they have a specific legislative mandate from the Congress to do so.

Third, the Congress should be sparing in mandating use of the SSN, and should do so only after full and careful consideration preceded by well advertised hearings that elicit substantial public participation. Such consideration should weigh carefully the pros and cons of any proposed use, and should pay particular attention to whether effective safeguards have been applied to automated personal data systems that would be affected by the proposed use of the SSN. (Ideally, Congress should review all present Federal requirements for use of the SSN and determine whether these existing requirements should be continued, repealed, or modified.)
Fourth, when the SSN is used in instances that do not conform to the three foregoing principles, no individual should be coerced into providing his SSN, nor should his SSN be used without his consent.

Fifth, an individual should be fully and fairly informed of his rights and responsibilities relative to uses of the SSN, including the right to disclose his SSN whenever he deems it in his interest to do so.

In accordance with these principles, we recommend specific, preemptive, Federal legislation providing:

(1) That an individual has a legal right to refuse to disclose his SSN to any person or organization that does not have specific authority provided by Federal statute to request it;

(2) That an individual has the right to redress if his lawful refusal to disclose his SSN results in the denial of a benefit, or the threat of denial of a benefit; and that, should an individual under threat of loss of benefits supply his SSN under protest to an unauthorized requestor, he shall not be considered to have forfeited his right to redress; and

(3) That any oral or written request made to an individual for his SSN must 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.

In addition, we recommend

(4) That the Social Security Administration undertake a positive program of issuing SSNs to ninth-grade students in schools, provided (a) that no school system be induced to cooperate in such a program contrary to its preference; and (b) that any person shall have the right to refuse to be issued an SSN in connection with such a program, and such right of refusal shall be available both to the student and to his parents or guardians;

(5) That there be no positive program of issuing SSNs to children below the ninth-grade level, either at the initiative of the Social Security Administration or in response to requests from schools or other institutions;

(6) That the Secretary limit affirmative measures taken to issue SSNs pursuant to Section 205(c)(2)(B)(i)(II) of the Social Security Act, as amended by Section 137 of Public Law 92-603, to applicants for or recipients of public assistance benefits supported from Federal funds under the Social Security Act; and

(7) That the Secretary do his utmost to assure that any future legislation dealing with the SSN be preceded by full and careful consideration and well advertised hearings that elicit substantial public participation.

With respect to organizations using the SSN, we recommend

(8) That any organization or person required by Federal law to obtain or record the SSN of any individual be prohibited from making any use or disclosure of the SSN without the informed consent of the individual, except as may be necessary to the Federal purposes for which it was required to be obtained and recorded. This prohibition should be established by a specific and preemptive act of Congress;

(9) That the Social Security Administration provide "SSN services" to aid record keeping only to organizations or persons that are required by Federal law to obtain or record the SSN, and then only as necessary to fulfill the purposes for which the SSN is required to be obtained or recorded;

(10) That the Social Security Administration provide "SSN services" to aid research activities only when it can assure that the provision of such services will not result in the use of the SSN for record-keeping and reporting activities beyond those permitted under recommendation (9), and then only provided that rigid safeguards to protect the confidentiality of personal data, including the SSN, are incorporated into the research design; and

(11) That specific, preemptive Federal legislation be enacted prohibiting use of an SSN, or any number represented as an SSN, for promotional or commercial purposes.