

FROM: United States Department of Health, Education & Welfare. 1973. Records, Computers, and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems, July, <http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm>

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

records for statistical-reporting and research purposes, deepens the anxieties of a public already suffused with concern about surveillance. If record-keeping systems and their data subjects were protected by strong safeguards, the danger of inappropriate record linkage would be small; until then there is a strong case to be made for discouraging linkage.

The report recommends that use of the Social Security number be limited to Federal programs that have a specific Federal legislative mandate to use the SSN, and that new legislation be enacted to give an individual the right to refuse to disclose his SSN under all other circumstances. Furthermore, any organization or person required by Federal law to obtain and record the SSN of any individual for some Federal program purpose must be prohibited from making any other use or disclosure of that number without the individual's informed consent.

The report recognizes the need to improve the reliability of the Social Security number as an instrument for strengthening the administration of certain Federally supported programs of public assistance. It also recognizes that issuing Social Security numbers to ninth-grade students in schools is likely to be consistent with the needs and convenience of young people seeking part-time employment and who need an SSN for Social Security and Federal income tax purposes. Accordingly, the Committee endorses the recommendation of the Social Security Task Force that a positive program of issuing SSNs to ninth-grade students in schools be undertaken. It does so, however, on the condition that no school system shall be induced to cooperate in such a program against its will, and that any person shall have a right to refuse to be issued an SSN in connection with such a program. The Committee recommends that there be no positive program of issuing SSNs to children in schools below the ninth-grade level; and that the 1972 legislation amending the Social Security Act to require enumeration of all persons who benefit from any Federally supported program be interpreted narrowly. Finally, the Committee recommends legislation to prohibit use of the Social Security number for promotional or commercial purposes.

The last chapter of the report contains an agenda of actions to be taken for implementing the Committee's recommendations, which are set forth in full below.

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.